A risk management model for securing virtual healthcare communities

Anargyros Chryssanthou

Hellenic Data Protection Authority,
Auditors Department,
1-3, Kifissias Avenue,
Ampelokipoi, Greece
Email: achrysanthou@dpa.gr

Iraklis Varlamis*

Harokopio University of Athens,
Department of Informatics and Telematics,
89, Harokopou St., Greece
Email: varlamis@hua.gr
*Corresponding author

Charikleia Latsiou

Hellenic Data Protection Authority,
Auditors Department,
1-3, Kifissias Avenue,
Ampelokipoi, Greece
Email: clatsiou@dpa.gr

Abstract: Virtual healthcare communities aim to bring together healthcare professionals and patients, improve the quality of healthcare services and assist healthcare professionals and researchers in their everyday activities. In a secure and reliable environment, patients share their medical data with doctors, expect confidentiality and demand reliable medical consultation. Apart from a concrete policy framework, several ethical, legal and technical issues must be considered in order to build a trustful community. This research emphasises on security issues, which can arise inside a virtual healthcare community and relate to the communication and storage of data. It capitalises on a standardised risk management methodology and a prototype architecture for healthcare community portals and justifies a security model that allows the identification, estimation and evaluation of potential security risks for the community. A hypothetical virtual healthcare community is employed in order to portray security risks and the solutions that the security model provides.

Keywords: information security; virtual communities; healthcare; ISO 27000 family of standards; risk assessment.

Reference to this paper should be made as follows: Chryssanthou, A., Varlamis, I. and Latsiou, C. (2011) 'A risk management model for securing virtual healthcare communities', *Int. J. Electronic Healthcare*, Vol. 6, Nos. 2/3/4, pp.95–116.

Biographical notes: Anargyros Chryssanthou is currently employed by the Hellenic Data Protection Authority as an ICT Auditor, where his duties include auditing the use of personal data by companies of the public and the private sector. He studied Applied Informatics in Athens University of Economics and Business. He holds an MSc in Information Security and Computer Crime from the University of Glamorgan (Wales – UK). His research interests include network security, cryptography, with special interest on steganography and computer forensics, where he is currently aiming on building a concise forensic methodology on investigating electronic crime in general and privacy violations in particular.

Iraklis Varlamis is a Lecturer at the Department of Informatics and Telematics of Harokopio University of Athens. He received his PhD in Computer Science from Athens University of Economics and Business, Greece. His research interests vary from data mining and the use of semantics in web mining to virtual communities and their applications. He has published several articles in international fora, concerning web document clustering, the use of semantics in web link analysis and web usage mining, word sense disambiguation using thesauruses, virtual communities in healthcare, etc.

Charikleia Latsiou is currently employed by the Hellenic Data Protection Authority as a Lawyer in the Auditors Department, where her duties include auditing the use of personal data by companies of the public and the private sector. She studied Law in Aristotle University of Thessaloniki. She received her PhD from the University of Freiburg (in cooperation with Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg). Her PhD thesis was on ‘Preimplantation Genetic Diagnosis – Legal and Ethical Issues’ (Präimplantations-diagnostik Rechtsvergleichung und bioethische Fragestellungen). Her research interests include bioethics, medical confidentiality and data protection.

1 Introduction

A virtual healthcare community allows its members such as doctors, patients and caregivers to communicate and collaborate in order to virtually manage the illnesses and improve the quality of patients’ life. The virtual environment removes distance and time barriers, enables patients to submit online requests for advice and share problems and solutions with other patients and facilitates doctors to cooperate with each other and supervise their patients. However, in order for the virtual healthcare community to thrive, community members need to *trust* each other and be confident for the *secure*, *reliable* and *lawful* operation of the community.

Virtual healthcare communities have some unique characteristics, which make the aforementioned targets hard to accomplish. They cross national borders and operate in a continuous basis; they are responsible for securing members’ medical data and are entrusted to preserve members’ anonymity. At the same time, they must guarantee the reliability of both participating members and submitted content. Under these circumstances, the smooth operation of such communities is a heavy duty for moderators and administrators.

The aim of this research is to study the security risks to healthcare communities and provide a risk management methodology based on widely accepted standards. For this reason, we capitalise on the adaptation of a standardised risk management model to virtual healthcare communities. The model iteratively identifies and evaluates many potential hazards and suggests new certification mechanisms, operational policies and functionalities that can improve the information communication tasks, strengthen the protection of the community assets and increase members' trust on the community.

The combination of different trust-enabling functionalities such as transparency, content quality control and access rights management strengthens users' trust towards the community (Ebner et al., 2004). Moreover, trust is achieved by following several repeating steps: (1) achieving an appropriate security level for medical data in terms of authentication and user's certification, (2) defining a strict user policy with roles, access rights and limitations among community members and (3) providing a flexible identification mechanism, which preserves anonymity while guaranteeing identity truthfulness. From a technical point of view, performing system maintenance, by means of internal and external auditing as well as vulnerability testing, is necessary for the stability of the community's infrastructure. A reputation system may help to elicit good behaviour, encourage knowledge sharing among individuals and strengthen members' bonds to the community.

The ISO 27000 family of information security standards offers a standardised methodology for securing the community infrastructure. More specifically, ISO/IEC 27001:2005 defines a methodology for planning and designing an Information Security Management System (ISMS), ISO/IEC 27002:2005 presents a code of practice for Information Security Management, ISO/IEC 27005:2008 provides a methodology for information security risk management and, finally, ISO/IEC 27799:2008 focuses on the specific needs of the e-health sector and provides a guide to health information practitioners on how to protect confidentiality, integrity and availability (CIA) of information and services. In addition to information security standards, the role of national laws and national or international data protection authorities is essential because they set the legal and regulatory boundaries that govern the community's operation. The authorities are responsible for checking whether the community securely handles members' personal and sensitive personal data and for guiding the community administrators on the necessary security level that must be achieved in the community's information systems' environment. The administrators of the community need to apply an information security risk management process in order to secure the community's information systems and achieve the required information security level.

The proposed model justifies a security-enabled architecture and follows a scenario-based validation process, which explains by means of hypothetical incident scenarios the controls selected in the security model proposed by Chryssanthou et al. (2009). All the scenarios are based on reported security violation incidents, which target the community assets and lead to loss of confidentiality, availability, integrity, etc. Limiting the borders of our hypothetical community at a national level, we emphasise on the legal implications of security incidents that involve sensitive medical data and present the legal obligations of the community towards the Hellenic Data Protection Authority (HDPA), according to Greek data protection law (Law 2472, 1997).

Related work on virtual healthcare communities, presented in Section 2, shows that security and trust are the two biggest issues for such communities. In order to provide a concrete security solution, the risk management model must be adapted to the specific requirements of the virtual healthcare community. For this reason, in Section 3 we describe the community structure focusing on the operational, regulatory and legal framework of the community. Section 4 applies the generic risk management model to the specific needs of the community and produces an applicable risk treatment plan. Emphasis is given to case-based analysis of potential community threats, which takes into account the legal implications behind security incidents. Finally, Section 5 presents the conclusions of this research.

2 Related research

Several commercial projects, which develop virtual healthcare communities for patient support, have attracted national or private funding. For example, Connecticut's General Life Insurance Company and Insurance Company of North America – CIGNA (Mondy and Torresi, 2008) has launched a virtual community for nutrition and healthcare, which is situated on a virtual island in Second Life[1] servers. The EU-funded project Saphire (Laleci et al., 2008) has integrated wireless medical sensor data with hospital decision support systems in an attempt to provide remote monitoring of patients at their homes. Research works on healthcare delivery (Demiris et al., 2004), patient–peer support (Schopp et al., 2004) and virtual disease management or medical research and collaboration through virtual medical communities have been found in the literature. In order to increase the quantity of medical information without burdening the patient, several sensor-based monitoring systems have been designed that allow continuous recording of patients' status such as CodeBlue (Lorincz et al., 2004), Scalable Medical Alert Response Technology (SMART) (Curtis et al., 2008) and MobiHealth (Jones et al., 2006).

The Health Information Trust Alliance[2] released a security framework for healthcare in March 2009, which is based on well-known standards and best practices such as ISO/IEC 27001:2005 and COBIT,[3] but it is only available to member organisations subsequent to paying a fee (Kaplan, 2009). The framework supports regulations such as the Health Insurance Portability and Accountability Act (HIPAA) (U.S. Congress, 2004) and aims in increasing the confidence of patients in the security of their information. In the Cassandra trust management system for medical communities (Becker and Sewell, 2004), access control is based on the member's role in the community, while each data owner is able to define the access rights on his/her personal data by using a prototype Role-Based Access Control (RBAC) model. Solving the security issues, which relate to the wireless or wired transmission of data (Ng et al., 2006), and addressing the legal and ethical issues concerning confidentiality of patient data (Stanberry, 1998) is a first step towards establishing a secure virtual healthcare community (Lee, 2009).

In such dynamic and data-rich environments, a holistic security approach (Wozak et al., 2007; Apostolakis et al., 2009; Chryssanthou et al., 2009) is needed in order to improve confidentiality and reliability and consequently increase community trust. In terms of a holistic solution, technological, organisational, human-related and other aspects must be examined in order to minimise the risk and potential damage for everyone (i.e. the patient, the doctor, the hospital, etc.). The approach should study the community structure, identify its assets as well as its pros (existing security controls) and cons (existing vulnerabilities) and record potential threats, in order to build a list of potential risks, which can be estimated and evaluated against selected criteria and will potentially lead to possible solutions by means of a well-formed risk treatment plan. A standardised methodology, e.g. based on ISO standards, should be employed for this purpose.

3 A virtual healthcare community for patient support

Virtual healthcare communities can be very broad covering patients, professionals, healthcare companies, medical associations, etc., and allowing information dissemination, professional training (communities of practice) and patient education (medical education communities). Self-supportive and patient-centric healthcare communities capitalise on patient empowerment through consultation, monitoring and intervention and are steadily gaining ground (Varlamis and Apostolakis, 2010). In such communities, healthcare service providers cooperate in order to support older members, patients or members with chronic conditions. Providers offer different types of healthcare services at different points in time, in this way bridging geographic distances and time constraints (Demiris et al., 2004).

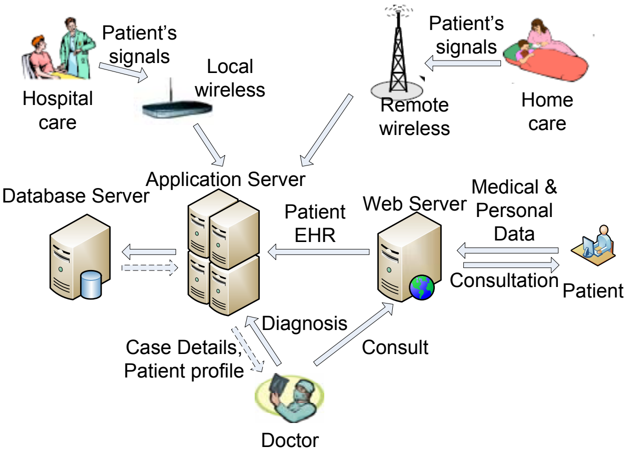
In the following subsections, we consider a hypothetical self-supportive virtual healthcare community, which focuses on patient monitoring and consultation, and adapt our security model to its specific requirements.

3.1 Hypothetical self-supportive virtual healthcare community model

The basis of our hypothetical community are active members that participate in everyday community activities and supportive members who work either in the foreground or in the background and guarantee the smooth operation of the community (see Figure 1). Active members are the patients, doctors as well as people with interest in the community issues such as patients' family members, researchers, etc. They have different roles depending on their needs and expertise. For example, patients and family members undertake facilitators' roles while healthcare professionals become moderators for discussion, consultation and content, as well as facilitators and mentors for the community members. Supportive members comprise IT experts who perform the technical administration of the community, the employees of the telecommunication service provider and the directors of the organisation, company or hospital that hosts the virtual community. They are the persons who do not actually participate in the community but play a key role in its secure operation. A coalition of one or more medical associations, hospitals or healthcare providers is responsible for the administration and the smooth operation of the community. The coalition, which we call as 'virtual hospital', recruits doctors and IT experts, assigns them roles and trains them to cater to the specific needs of the virtual community. Patients who join the community must upload their medical records on to the community servers and have the right to grant or revoke access privileges to any individual, doctor, nurse or caregiver.

Everyday interactions inside the healthcare community are presented in Figure 1. Health status signals are collected using wireless sensors and/or wired devices and are stored in the community servers for future reference and analysis. Patient members are also able to ask for advice, diagnosis, treatment suggestion, etc. by using the community portal communication services (e.g. e-mails, forums, etc.). Each doctor replies to patients' requests but also provides consultation based on monitored patients' medical status signals. The virtual hospital keeps record of patients' profiles and history, doctors' diagnoses and of all interactions between community members.

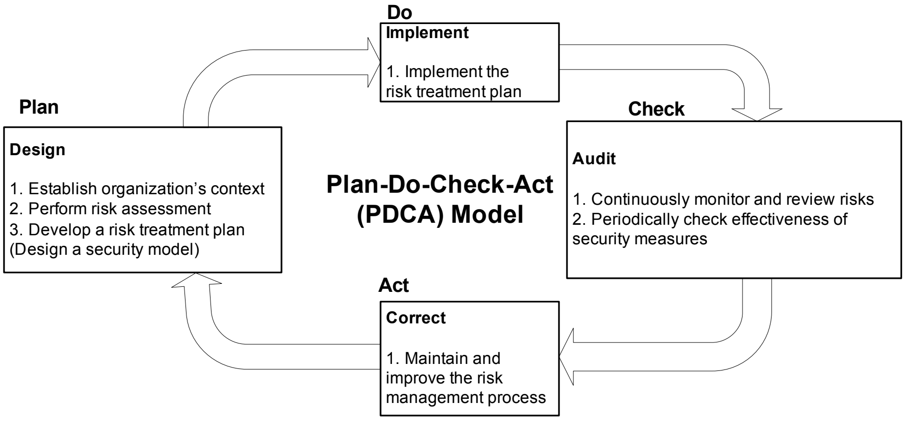
Figure 1 Overview of the community interactions (see online version for colour)



3.2 Information security risk management cycle

Information security risk management is a continuous process for any information system. In our community, we start with a basic community infrastructure, with minimum security controls in place, and follow the information security risk management methodology, described in ISO/IEC 27005:2008. This methodology is part of a continuous cycle of procedures (depicted in Figure 2), which repeats itself as an organisation evolves and depends on the legal and operational environments, in which the organisation operates. In the first step (Plan) of this repetitive process, the community context is defined along with the critical assets and potential risks. Risks are assessed and prioritised and a risk treatment plan is formed. In the second step (Do), the risk treatment plan is implemented and subsequently (in the third step – Check) is checked for its effectiveness. The fourth step (Act) comprises all the corrective actions that maintain and improve the risk management process.

Figure 2 Information security risk management cycle (combining ISO/IEC 27001:2005 and ISO/IEC 27005:2008)

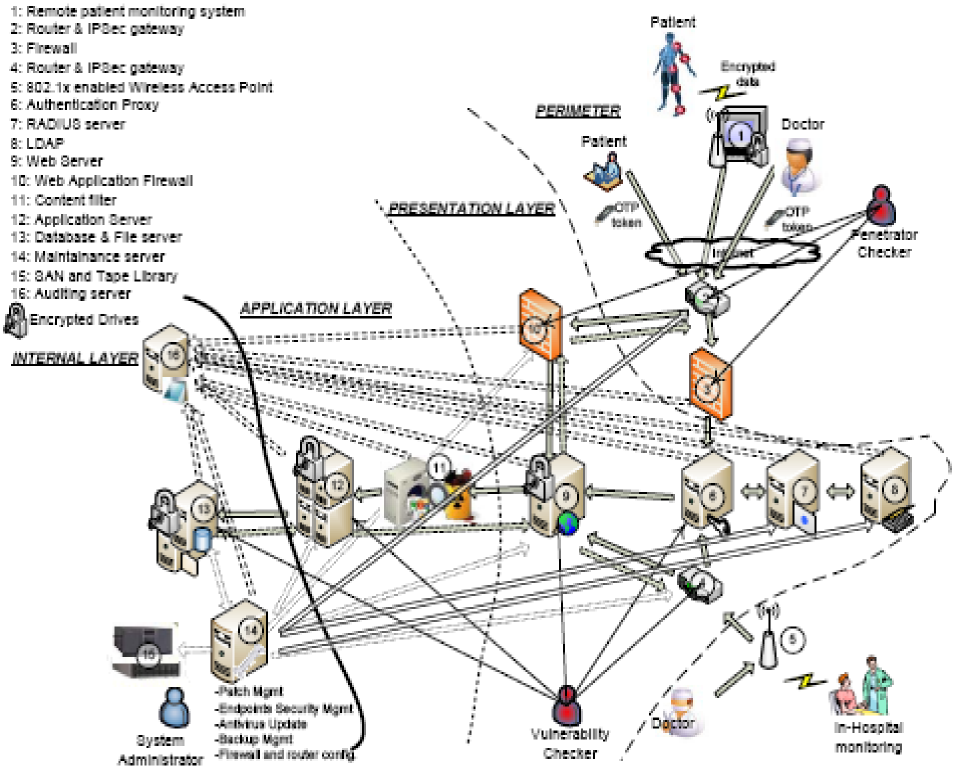

Do
Implement
1. Implement the risk treatment plan
Plan
Design
1. Establish organization's context
2. Perform risk assessment
3. Develop a risk treatment plan (Design a security model)
Plan-Do-Check-Act (PDCA) Model
Check
Audit
1. Continuously monitor and review risks
2. Periodically check effectiveness of security measures
Act
Correct
1. Maintain and improve the risk management process

3.3 Security-enabled architecture

We now describe the 'Plan' phase of the methodology, which leads to the design of the security-enabled architecture that we presented in Chryssanthou et al. (2009) and that is depicted in Figure 3. The architecture is multi-layered and assumes that the sensitive community information is stored in the secured internal layer, which guarantees software updates, data backups, etc. The application and presentation layers are responsible for the communication of information to the community members who access the community portal from a hospital or from home.

We focus on data security and ignore the social, medical or other aspects of a healthcare community. We perform a holistic security analysis concerning the communication, storage and access of sensitive medical data and cover different perspectives such as technical, operational and legal. Virtual communities are usually transnational, and the legal framework on data security violations differs from a country to another country. In order to provide a concrete solution and avoid conflicts from different national legal frameworks, we presuppose a centralised community repository of data, which resides in a European country, more specifically in Greece, and consequently focus on the legal framework in Greece.

Figure 3 Security-enabled architecture (see online version for colour)



4 Applying a security risk management model to a virtual healthcare community

According to ISO/IEC 27005:2008, the plan phase comprises: (a) context establishment, (b) risk assessment, (c) risk treatment and (d) risk acceptance.

4.1 Context establishment

Establishing the context of the community means setting the goal of the information security risk management methodology, setting basic criteria (for risk evaluation, impact and risk acceptance), defining scope and boundaries and identifying the organisation, where the methodology is applied. In Section 3, the functionality of a 'virtual hospital', which is located in Greece, was described. The stakeholders (such as doctors, patients, etc.) were identified and the roles of all the parties inside the community were briefly described.

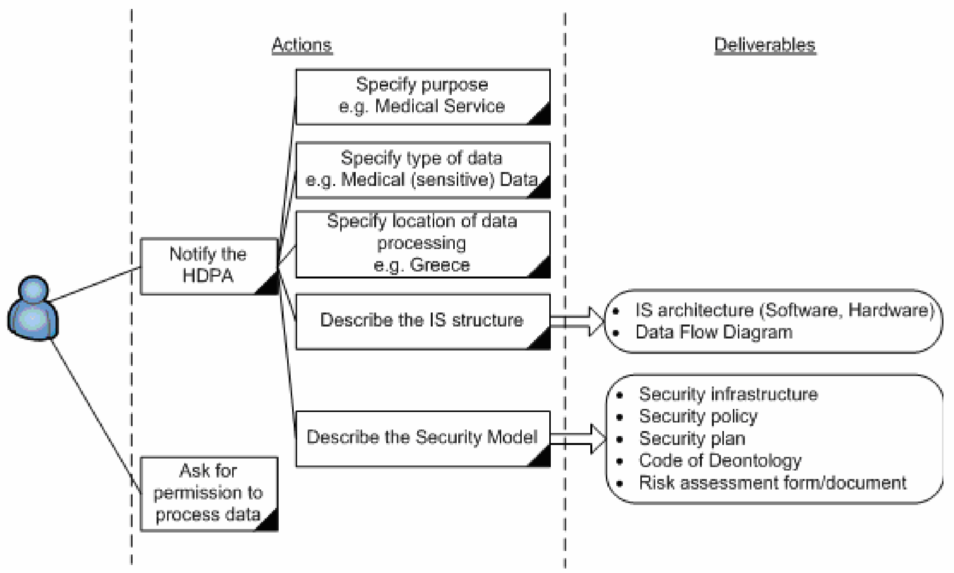
The 'virtual hospital' processes medical data; thus, it abides to data protection laws, which are applied to personal data or to cases where appropriate security measures are not implemented. In order to examine the legal and regulatory requirements of 'data security', we must define the meaning of geographical boundaries for the community. Since the community resides in a country of the European Union (EU), it abides to the EU opt-in model for all personal data, which assumes that all personal information is classified until their owner grants access on them (EU Council, 1995). According to the EC directive on the protection of individuals with regard to the processing of personal data (EU Council, 1995), only health professionals can access medical information and they are responsible for protecting confidentiality. According to the Recommendation (97) 5 (EU Council, 1997), medical data can be collected without user consent, only for preventing a real danger or in the case of a criminal offence.

Since the 'virtual hospital' is located in Greece, it abides to the Greek Data Protection Law (Law 2472/1997), which is in accordance to the European Data Protection Directive (EU Council, 1995). According to the Greek Law, medical data are sensitive data (Article 2b), the 'data controller'[4] needs to notify the HDPA on processing personal data (Article 4) and subsequent to the HDPA's permission only healthcare professionals are allowed to process medical data (Article 7/1d) following the Greek Medical Code of Deontology (Law 3418/2005). Data processing is allowed only if this is necessary for medical prevention, diagnosis, care or management of healthcare services. Under an amendment of the law in 2006 (Law 3471/2006), Article 10, Paragraph 3 states that the data controller must take appropriate security measures in order to protect privacy of sensitive data.

The data administrator of the community is obliged to notify the HDPA on processing sensitive medical data and request permission for this process. The notification submission process is depicted in Figure 4. The rectangles correspond to actions that should be carried by the community administrator(s), and the rounded rectangles show the deliverables of each action. The administrator(s) of the community must notify the HDPA that they process medical data, which are sensitive data, for the purpose of providing medical services, and that they reside in Greece. The administrators must also inform the HDPA on the architecture of their information system and the data flow in it. Finally, they should submit a detailed security report, which contains the security infrastructure of the community, the security policy, the security plan, the Code of Deontology and the latest performed risk assessment. They can also optionally submit their secure destruction policy document. With all these completed, the data controller (i.e. the virtual community operating authority) has completed its notification submission and waits for it to be examined and approved by the HDPA.

The scope of applying the risk management methodology is to achieve legal compliance and to ensure that 'virtual hospital' achieves CIA with regard to all of its valuable assets. Beyond the legal notification obligation, possible legal issues that might arise could involve improper use of patient data, selling data to insurance companies and use of medical data for other than the notified purpose. In case of illegal processing of data, if the data controller resides in Greece, then s/he is subject to penal, civil and administrative sanctions according to Articles 21–23 of the Greek Data Protection Law (Law 2472/1997).

Figure 4 The HDPA notification submission process (see online version for colour)


Actions
Deliverables
Specify purpose e.g. Medical Service
Specify type of data e.g. Medical (sensitive) Data
Specify location of data processing e.g. Greece
Notify the HDPA
Describe the IS structure
• IS architecture (Software, Hardware)
• Data Flow Diagram
Describe the Security Model
• Security infrastructure
• Security policy
• Security plan
• Code of Deontology
• Risk assessment form/document
Ask for permission to process data

The scope of applying the risk management methodology is to achieve legal compliance and to ensure that 'virtual hospital' achieves CIA with regard to all of its valuable assets. The criteria that will be used in order to assess the impact of any given risk will be:

- level of classification of the information asset
- breaches of information security (with regard to CIA)
- loss of business or financial value
- damage of reputation
- breaches of legal requirements.

Similarly, criteria that will be used in order to evaluate the identified risks will be:

- criticality of information assets
- business impact (financial costs, negative consequences for reputation and issues of stakeholders' trust)
- consequences regarding CIA
- legal requirements
- patient health and patient protection.

In conclusion, we must clarify that a security model by itself is not a panacea against all security threats or that a secure system remains secure forever. Although they cannot guarantee avoidance of data loss or data leakage, a concrete legal framework, a well-defined compliance evaluation process and routine checks are all tools that enforce liability over security incidents and force the community owners to capitalise on data and systems security.

4.2 Risk assessment

Risk assessment is the overall process of risk analysis and evaluation. Risk analysis comprises identification of risks and estimation of their impact to the organisation. During the identification step, both assets and risks are recorded: assets can be humans, technical infrastructure, pieces of information, critical processes, etc., whereas risks can be internal or external threats, which exploit technical or operational vulnerabilities. In this same step, the available security controls are recorded. Risk estimation defines the criticality level, the possibility of each risk and the potential consequences for the organisation. Finally, risk evaluation examines each identified risk against selected legal, operational and organisational criteria, which have been selected beforehand, and sets the priorities for the risk treatment plan that follows.

According to the methodology defined in ISO/IEC 27005:2008, the information security specialists of the 'virtual hospital' are responsible to: (a) locate the assets of the virtual community, giving emphasis to patients' sensitive medical data, (b) identify potential risks by analysing reported incidents that relate to the exposure, damage or loss of patient information, (c) assess the identified risks and form a risk treatment plan that selectively incorporates new security controls in the community's information security model.

4.2.1 Risk identification

Risk identification is the first step of the risk assessment model and refers to the recording of: (a) valuable community assets, (b) potential community threats, (c) existing security controls, (d) detected vulnerabilities and (e) consequences of potential incident scenarios with regard to the CIA. Among the long list of possible incident scenarios, we focus on those which mostly affect patients and their medical data and examine in detail the following scenarios: (a) patient information stealing, (b) social engineering acts and (c) malware attacks. Each scenario corresponds to a potential risk for the virtual healthcare community. A summary of assets, vulnerabilities, security controls and consequences that relate to the scenarios is presented in Table 1. The details are discussed in the following sub-sections.

Table 1 Incident scenarios and identified risks

Incident scenarios/ potential threats	*Assets in risk*	*Existing security control*	*Exploitable vulnerabilities*	*Potential consequences*
Patient information stealing	(1) Information repository (e.g. hard disc) (2) Data exchange application (3) Medical data	Security guards outside the server rooms	(1) Unencrypted hard drives (2) SQL injection vulnerability (3) Absence of an endpoint security solution	(1) Data loss (2) Issues of trust (3) Loss of work time (4) Financial cost (5) Loss of reputation (6) Legal sanctions
Social engineering act	(1) Humans (2) Means of authentication (3) Medical data	–	Absence of an access and behaviour policy	Same as (1) to (6) above
Malware attack	(1) Servers (2) Backbone infrastructure (3) Users’ equipment	Antivirus suites	Outdated and not frequently updated antivirus suites	Same as (1) to (6) above with (7) Loss of functionality

4.2.1.1 Community assets

Identified assets are the active members of the community, medical data and the internal structure of the community, which consists of information systems and physical premises. Patients and their sensitive medical data are the most valuable assets in our community and must be protected from unauthorised and improper use. Protection of assets follows the traditional CIA model of security: Data and systems must remain *Confidential*, maintain their *Integrity* and remain constantly *Available*. The second column of Table 1 summarises the assets which are in risk in each of the three examined scenarios. Each asset can be classified according to its importance into three different levels: low, medium or high. These classifications derive from the request for each CIA principle, which can be low, medium or high for an asset. If a quantitative assessment of assets against each of the three CIA principles is possible, then a value is estimated for each asset in risk. A classification (valuation) of assets, with regards to CIA, affected by the examined scenarios is depicted in Table 2.

Table 2 Classification of assets

Asset	*Confidentiality*	*Integrity*	*Availability*	*Classification of asset*
Information repository (e.g. hard disc)	High	High	High	High
Data-exchange application	Medium	High	High	High
Medical data	High	High	High	High
Humans	Medium	Medium	Medium	Medium
Means of authentication	High	High	High	High
Servers	High	High	High	High
Backbone infrastructure	Medium	Medium	Medium	Medium
Users' equipment	Medium	Medium	Medium	Medium

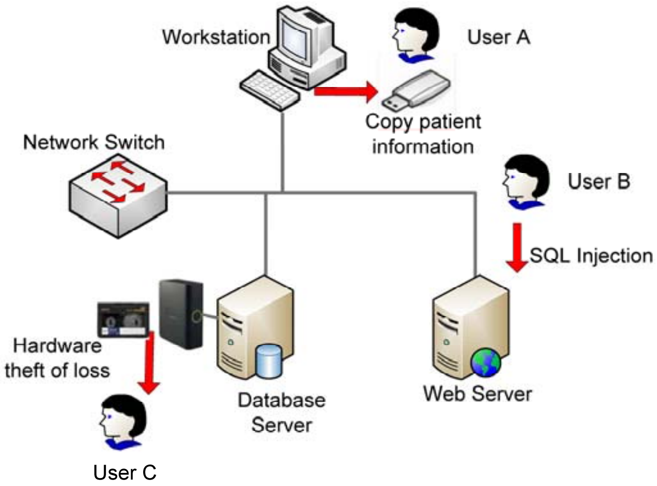
4.2.1.2 Community threats

Information sharing between the members of virtual healthcare communities raises concerns about privacy and safety of medical data. Previous studies in healthcare information systems show that threats can be either accidental events or deliberate actions (Kahn and Sheshadri, 2008). Security risks either start from technical vulnerabilities or from security-unaware humans (Samy et al., 2010). The technical aspect of threats relates to malicious attackers, system users or insiders that exploit hardware or software weaknesses. The social engineering aspect relates to gullible users who fall victims of social engineering attacks. Both types of threat target the information repository and the operational infrastructure of the virtual healthcare community.

The long list of threats presented in ISO 27799:2008 contains among others: (a) accidental system failures (e.g. power, network or hardware failure, software bugs, etc.), which may lead to loss or leak of medical data and temporary or permanent denial of medical services, (b) unintentional malware attacks, network infiltration or wilful damages by outsiders that target the system's vulnerabilities, (c) acts of human error and system resources' misuse, (d) social engineering attacks, (e) natural disasters, etc. According to Samy et al. (2010), the most critical threats for health information systems are system failures (power, network, hardware and software), acts of human error and technological obsolescence. In our study, we focus more on threats that emanate from human acts than from technical faults, adapt the most critical threats to the specific requirements of virtual healthcare communities and explain how the security risk management model treats them. More specifically, we examine in detail the following threats: (a) patient information stealing, (b) social engineering acts and (c) malware attacks.

In the information-stealing scenario, a skilful internal or external user steals sensitive information in order to perform fraud, identity theft, etc., and achieve personal profit. It can be an individual internal user, with physical access to the community servers, who copies data in a portable drive (user A in Figure 5), a malicious external user who performs SQL-injection (an unauthorised execution of code to the database) through an unsecured application of the community portal and manages to draw illegitimate information from the database (user B in Figure 5) or a community data repository (e.g. a hard disc, laptop, backup medium) which is stolen by an outsider or lost by an insider (user C in Figure 5).[5]

Figure 5 Information stealing (see online version for colour)



In the social engineering attack scenario, a malicious outsider gains access to an organisation's infrastructure by manipulating people working in the organisation in a way that they happily reveal information which is otherwise confidential, such as social security number, password, etc.[6] Such an attack could come from anywhere. For example, a person posing as a technician might call and persuade a user to reveal his password as part of a security maintenance procedure.

In malware attacks, harmful software (such as worm, Trojan horse, Rootkit, spyware, adware, etc.) is installed in the community portal servers.[7] The software can be installed accidentally, when an administrator installs infected software on the community servers or when he visits an infected web page from one of the community servers. Depending on its payload, the malware can even spread itself across the network to machines suffering from the same security vulnerability and quickly lead to disruption of the community's portal operation.

4.2.1.3 Security controls

The protection of a community against potential threats is the existing security controls, so the installed security controls, their implementation details and usage status must be recorded first (column 3 of Table 1). With regard to physical security, our community's infrastructure is currently protected by security guards outside the server rooms. As far as logical security is concerned, the servers are equipped with outdated antivirus suites that are not updated frequently, while no endpoint security solution is in place to guard against the use of portable media for unauthorised purposes.

4.2.1.4 Vulnerabilities

A threat becomes a real danger for the community if it manages to exploit existing vulnerabilities. For this reason, the identification of vulnerabilities is an important task and should be performed in a constant basis. Vulnerabilities relate to the human factor (personnel), the organisational and management routines, the technological infrastructure and the physical premises of the organisation. The absence of an access control policy, the sharing of passwords among different users and the lack of a secure data transmission method are some examples of vulnerabilities. Although the existence of vulnerabilities does not necessarily mean harm, all identified weaknesses should be properly treated or else should be constantly monitored. The fourth column of Table 1 summarises the vulnerabilities that can be exploited in each scenario.

In the information stealing or loss threat, the vulnerabilities relate to the ability to export data from the community's servers. The absence of an endpoint security solution guarding the use of portable media favours the theft of information by an insider by means of a portable drive. In the case of data stealing through SQL injection, the vulnerability lies in the data exchange applications and mainly in the input validation process. Finally, the existence of unencrypted hard drives containing sensitive data works in advantage of an outsider who manages to infiltrate the community perimeter (by means of physical presence).

The vulnerability in the social engineering threat is the human factor. The absence of an access and behaviour policy favours the social engineer as the users are not well educated concerning information security and are, thus, more content to give away their credentials to such an attacker.

The usage of outdated and not frequently updated antivirus suites makes the community's servers susceptible to malware attacks because the antivirus suites are not equipped (with proper signatures) to handle new viruses and are unable to employ methods, such as heuristic analysis, to deal with previously unknown computer viruses.

4.2.1.5 Consequences

The final step of the identification phase comprises the identification of consequences to the organisation. The incident scenarios are tested against the existing security controls of the virtual community and the consequences are recorded. These consequences (column 5 in Table 1) include: (a) technical amendments, since new security controls must be implemented as countermeasures to security violation threats, (b) additional financial cost, as these security measures are not free and (c) ethical and legal issues (Clause 7.3 in ISO/IEC 27005:2008).

Information stealing is in fact a data breach incident, which is subject to civil, administrative and penal sanctions imposed from data protection laws. The consequences of such an incident can be legal, ethical, business like and technical. A user that steals information by means of a portable device or an SQL-injection attack that steals patient's medical data causes issues of trust in the community and decreases the community's reputation. Community administrators and technical staff lose work time in the investigation of the data breach incident and the coalition faces financial costs, both from legal sanctions from the data protection authorities and from the effort to address the exploited vulnerability or to correct the damage. In a real-world incident, the Royal Bolton Hospital, Bolton, England, reported the theft of a computer that contained the private details of 350 chest patients in January 2008.[8] The hospital contacted all patients to inform them of the theft, but insisted that all information is data-protected and cannot be accessed by anyone other than the relevant hospital staff. In order to improve security, the hospital recalled all its computers and laptops so that vital security software can be installed, which will encrypt patients' details. Additionally, encryption software was installed on all memory sticks and pen drives. Finally, all information was planned to be transferred to a central server and hosted in a secure storage network – rather than on individual hard drives. The hospital invested, as a consequence of the incident, an additional sum of £200,000 in order to increase its information security. In a similar incident, involving theft of a computer containing medical data in Lucile Packard Children's Hospital at Stanford, California, USA, the hospital was fined with US$ 250,000 from California's Department of Public Health for late reporting of the incident.[9]

In a social engineering attack, where a skilful attacker manages to authenticate as a doctor and participate in the community, the confidentiality of medical data is threatened. The attack can raise issues of trust because a patient might be given falsified advice and have his/her data intercepted. Similar consequences to the information-stealing scenario also apply in this case because time is needed to investigate the security incident and legal penalties may be imposed.

A malware attack may result in loss of data, malfunctioning or denial of medical services, system unavailability, etc. In a real-world incident, in 2008, three London hospitals were hit by a virus. The virus infection resulted in ambulances being redirected to neighbouring hospitals, while lab testing and imaging were performed by using pen and paper backup systems.[10] The particular incident affected the availability of systems causing among others, issues of trust, loss of functionality, financial costs and loss of reputation. Such an incident could also cause loss of data and legal sanctions.

4.2.2 Risk estimation

Risk estimation examines the severity and likelihood of each identified risk. It associates the consequences of each incident scenario with the assets that are in risk and estimates the impact to the community. Based on facts from related reports or previous system audits, risk estimation qualitatively measures the likelihood of a risk (low, medium and high) by studying. The output (column 2 in Table 4) is a qualitative estimation for each identified risk.

The analysis of the risk estimation for the information steeling scenario is depicted in Table 3. The consequences (depicted in column 5 of Table 1) are evaluated per asset. According to a study of the Ponemon Institute,[11] 60% of 65 health organisations in the

USA suffered at least one data breach incidence per year in 2008–2009 with the main cause being stolen devices (41%). Thus, the likelihood of patient information stealing is high. According to the same survey, the economical impact of data breaches was 1 million US$ per year, which is a high financial cost and the churning rate was 87 patients per breach, which is also a damage in reputation with high economical impact (4.5 million US$ per year). Combining the likelihood of event with the multiple costs of each consequence, we estimate that the level of risk for the patient information stealing scenario is '*high*'.

Table 3 Patient information stealing – assessment of consequences

Affected asset	*Classification of affected asset*	*Breaches of CIA*	*Financial cost*	*Reputation damage*	*Breaches of legal requirements*	*Value of consequence*
Information repository (e.g. hard disc)	High	High	High	High	High	High
Data exchange application	High	High	Medium	Medium	Medium	Medium
Medical data	High	High	High	High	High	High

In the social engineering scenario, the value of consequence per affected asset is: (a) medium for human and means for authentication and (b) high for medical data. According to Medlin et al. (2008), the likelihood of event for such a scenario is medium, because medical personnel is always obliged to help; thus, it is more susceptible to a skilful social engineer. Moreover, according to Medlin et al. (2008), 73% of healthcare employees shared their passwords with a co-worker or a friend even after receiving password protection training. Thus, the level of risk assigned to this scenario is '*medium'*.

In the malware attack scenario, the value of consequence per affected asset is: (a) high for servers and (b) medium for backbone infrastructure and user equipment. Based on incidents, such as the one presented earlier and the global statistics on malware activity, the likelihood of a malware attack is deemed high. Thus, the level of risk of the malware attack scenario is '*high'*.

4.2.3 Risk evaluation

In the risk evaluation phase, all the identified risks and their consequences are evaluated using selected criteria. The criteria are selected beforehand and can be legal, operational and organisational. In the virtual hospital's case, the criteria were selected in the context establishment phase and they included criticality of information assets, business impact (financial costs, negative consequences for reputation and issues of stakeholders' trust), consequences regarding CIA, legal requirements, patient health and patient protection. The evaluation takes as input the risk information from the estimation phase and produces a risk impact matrix that provides a score for each identified risk. The administrators of the virtual hospital examine the risk impact matrix and take business decisions that prioritise the treatment of specific risks (column 3 of Table 4). Based on the results of the risk evaluation process, they decide whether the risk should be treated immediately, in due time or accepted.

Table 4 Risk estimation, evaluation and treatment

Incident scenarios/potential threats	*Risk estimation*	*Risk evaluation*	*Risk treatment*	
			Control to be implemented	*Selected ISO 27001:2005 control*[a]
Patient information stealing	High	High	(1) Endpoint security solution (2) Specialised input filtering modules, web application firewall in the (presentation layer), authorisation (application layer) (3) Encryption of media (e.g. hard drives) + hardware tokens + physical security measures (e.g. access card systems)	(1) Management of removable media (A.10.7.1) (2) Controls against malicious code (A.10.4.1), Input data validation (A.12.2.1) (3) Cryptographic controls (A.12.3), Physical and environmental security (A.9)
Social engineering acts	Medium	Medium	(1) Hardware tokens and strong passwords + community roles+ overall access and behaviour policy (2) Auditing (3) Physical security measures	(1) Access control (A.11), cryptographic controls (A.12.3) (2) Audit logging (A.10.10.1), monitoring system use (A.10.10.2)[b], protection of log information (A.10.10.3), administrator and operator logs (A.10.10.4) (3) Physical and environmental security (A.9)
Malware attacks	High	Medium	(1) Up-to-date antivirus suites (2) Patch management suite (3) Disaster recovery plan	(1) Controls against malicious code (A.10.4.1) (2) Technical vulnerabilities management (A.12.6.1) (3) Business continuity management (A.14.1)

Notes: [a] For each control in this column, the name of the control is written and the number of the control follows in parentheses. Each control corresponds to the actual security control in the previous column. A complete list of security controls that are applicable to any kind of organisation structure can be found in ISO 27001:2005 (Annex A) and in ISO 27002:2005.

[b] Clause 7.2 in ISO/IEC 27799:2008.

Judging by the overall identification of the presented risks and their components, patient information stealing is deemed a high risk because it affects a classified asset (medical data) and it is rated high in all evaluation criteria that were selected beforehand. Thus, the appropriate measures must be taken immediately.

Social engineering attacks might have a huge impact, if the credentials of an administrator are stolen, but usually it is of lesser impact because the attacker usually gains access to limited amount of information (e.g. a patient's account and his medical data). Thus, this type of attack is rated low on business impact, medium with regard to CIA and medium on legal requirements (it asserts legal sanctions). Since social engineering attack affects medium to high-valued assets, its overall risk evaluation is medium and measures must be taken in a second phase.

Finally, malware attacks can have a huge impact, medium score on legal requirements, high on business impact and medium with regard to CIA because this type of attacks affects medium to high-valued assets. Hence, its overall risk evaluation is medium and measures must be taken in a second phase.

4.3 Risk treatment plan

Upon completion of a risk assessment, a risk treatment plan must be formed (Clause 9 in ISO/IEC 27005:2008). The plan must explain the selection of security controls in relation to the identified risks and with reference to the community portal architecture (Figure 3). Columns 4 and 5 of Table 4 provide a summary of the controls that must be implemented in accordance to ISO 27001:2005 premises.

Data loss due to theft or loss of storage media can be avoided using an endpoint security solution, which blocks or controls access to portable media devices by users. The lost portable media device is then useless because it is not allowed to copy sensitive data in portable devices. The existence of physical security measures (such as access card systems, access codes, security cards, etc.) makes it even harder to access the community's IT room or steal a backup tape from its physically secure storage location. In a remote attempt for data theft (e.g. via SQL injection), the use of specialised input filtering modules and of a web application firewall in the presentation layer is necessary. Web attack signatures, identification of SQL injection characters and dynamic profiling of data traffic constitute the first layer of defence against remote information-stealing attacks. Authorisation at the application server level adds an extra obstacle to illegal data access. The use of encryption for every storage media and the requirement for hardware tokens impede an internal attacker from stealing such a media.

An authentication method that combines hardware tokens and strong passwords, along with a registration on a certification authority, diminishes the possibility of a malicious user obtaining access to the community through a social engineering attack. The e-token device adds an extra authentication layer because the attacker who learns something a user knows (e.g. password) is still denied access to the community's systems until s/he manages to convince the user to hand on his e-token device. Even when a social engineer convinces users to hand on sensitive data, content moderators can act as a second certification authority, preventing the fraudulent users' actions and protecting users from deception. Auditing mechanisms can give an audit trail to the social engineer. The existence of an overall access and behaviour policy educates the user and prevents him/her from being an easy prey to social engineering attacks. Finally, physical security measures deter attackers from entering the community's IT room unaccompanied and gaining physical access to sensitive data.

The first step against malware attacks or external system attacks is therefore to install and constantly update antivirus suites and protect both critical systems and end-users' systems. The second step is to properly configure a patch management suite which regularly updates the community software and guards against new found vulnerabilities. In case of a 'zero-day exploit',[12] a disaster recovery plan must be able to function properly, in order to restore the attacked community's servers with the minimum downtime.

Based on the selected controls, a security model for the community is formulated. Along with this security model, the architecture of the community's ISMS is designed. Multitier architectures (Maji et al., 2008; Chryssanthou et al., 2009) can solve authentication and security issues of the medical community and strengthen the protection of medical data against improper use, unauthorised access or accidental loss.

5 Conclusions

The design of a secure and trustful community is a difficult though interesting task, which should be preferably performed by following standardised procedures. In this direction, this paper capitalises on widely accepted security standards (the ISO 27000 family of standards) and provides a roadmap for developing a secure solution. In this dynamic environment, new applications are added, thus causing the appearance of new exploits, creating new threats and new attack forms. Security and trust management requires careful handling of all the aforementioned issues and continuous maintenance of the community infrastructure. In this work, we presented the details on the application of the risk management model in a healthcare community with respect to several security violation incidents, frequently reported in healthcare. Security in healthcare communities is not a simple task, and there is not a single solution or remedy. The research presented in this paper provides a roadmap for developing a secure solution, which will soon deteriorate if the suggested risk management model is not iteratively repeated. With well-defined procedures and workflows, this standardised methodology achieves a secure environment for the healthcare community and allows medical professionals and patients to act inside the community with minimum risk for their valuable assets.

This study performed a structural analysis of the virtual community's supporting infrastructure and has been based on risk management examples reported in the literature and on a standardised risk management methodology. The evaluation of risks was based on reported incidents and statistics. The next steps of this work would comprise the prototype implementation of the security model for a healthcare community and an evaluation that will cover all possible attack scenarios. In this implementation, the risk management model will be tested in a real-world scenario, risks will be evaluated by a team involving healthcare professionals and the risk management decisions will be taken by real healthcare community owners. This implementation is expected to demonstrate the abilities of the suggested model, to uncover its inefficiencies and to help in improving its overall effectiveness.

References

Apostolakis, I., Chryssanthou, A. and Varlamis, I. (2009) 'A holistic perspective of security in health related virtual communities', in Lazakidou, A. and Siassiakos, K. (Eds): *Handbook of Research on Distributed Medical Informatics and E-Health*, IGI Global, Hershey, PA, USA, pp.367–381.

Becker, M.Y. and Sewell, P. (2004) 'Cassandra: flexible trust management applied to electronic health records'. Paper presented at the *17th IEEE Workshop on Computer Security Foundations*, 28–30 June, Asilomar Conference Center, Pacific Grove, CA, USA.

Chryssanthou, A., Latsiou, C. and Varlamis, I. (2009) 'Security and trust in virtual healthcare communities', Paper presented at the *2nd international Conference on Pervasive Technologies Related To Assistive Environments* (*PETRA 09*), 9–13 June, Corfu, Greece.

Curtis, D.W., Pino, E.J., Bailey, J.M., Shih, E.I., Waterman, J., Vinterbo, S.A., Stair, T.O., Guttag, J.V., Greenes, R.A. and Ohno-Machado, L. (2008) 'SMART – an integrated, wireless system for monitoring unattended patients', *Journal of the American Medical Informatics Association*, Vol. 15, No. 1, pp.44–53.

Demiris, G., Parker, O.D., Fleming, D. and Edison, K. (2004) 'Hospice staff attitudes towards telehospice', *American Journal of Hospice and Palliative Care*, Vol. 21, No. 5, pp.343–348.

Ebner, W., Leimeister, J.M. and Krcmar, H. (2004) 'Trust in virtual healthcare communities: design and implementation of trust-enabling functionalities', Paper presented at the *37th Hawaii International Conference on System Sciences (HICSS 04) – Track 7*, 5-8 January, Big Island, Hawaii.

European Council (1995) 'Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data' (N.I. 281/31-23/11/1995), Official Journal of the European Communities.

European Council (1997) *Explanatory Memorandum to Recommendation No. R(97) 5 of the Committee of Ministers to Member States on the protection of medical data*. (Adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting of the Ministers' Deputies). Available online at: http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/EM_R(97)5_EN.pdf

ISO/IEC 27001 (2005) *Information Technology – Security Techniques – Information Security Management Systems – Requirements*, 1st ed., 2005-10-15.

ISO/IEC 27002 (2005) *Information Technology – Security Techniques – Code of Practice for Information Security Management*1st ed.

ISO/IEC 27005 (2008) *Information Technology – Security Techniques – Information Security Risk Management*, 1st ed., 2008-06-1.

ISO/IEC 27799 (2008) *Health Informatics – Information Security Management in Health Using ISO/IEC 27002*, 1st ed., 2008-07-01.

Jones, V.M., van Halteren, A.T., Dokovski, N.T., Koprinkov, G., Peuscher, J., Bults, R., Konstantas, D., Widya, I.A. and Herzog, R. (2006) 'Mobihealth: mobile services for health professionals', in Istepanian, R.S.H., Laxminarayan, S. and Pattichis, C.S. (Eds.): *M-Health Emerging Mobile Health Systems*, Springer, New York, NY, USA, pp.237–246.

Kahn, S. and Sheshadri, V. (2008) 'Medical record privacy and security in a digital environment', *IEEE Journal of IT Professional*, Vol. 10, No. 2, pp.46–52.

Kaplan, D. (2009) 'Group unveils first-of-its-kind standard to secure patient data', *SC Magazine*. Available online at http://www.scmagazineus.com/group-unveils-first-of-its-kind-standard-to-secure-patient-data/article/128168/ (accessed 20 June 2011).

Laleci, G.B., Dogac, A.., Olduz, M., Tasyurt, I., Yuksel, M. and Okcan, A. (2008) 'SAPHIRE: a multi-agent system for remote healthcare monitoring through computerized clinical guidelines', in Annicchiarico, R., Cortés, U., Urdiales, C. (Eds): *Agent Technology and e-Health. Whitestein Series in Software Agent Technologies and Autonomic Computing*, Birkhäuser, Basel, Switzerland, pp.25–44.

Law 2472 (1997) *Protection of Individuals from Personal Data Processing*, Pub. L. No. 2472, Greece.

Law 3418 (2005) *Medical Code of Deontology*, Pub. L. No. 3418, Greece.

Law 3471 (2006) *Protection of Personal Data and Privacy in the Telecommunications Sector – Amendment of Law 2472/1997*, Pub. L. No 3471, Greece.

Lee, C.Y. (2009) 'Understanding security threats in virtual worlds', Paper presented at the *15th Americas Conference on Information Systems (AMCIS)*, 6–9 August, San Francisco, USA.

Lorincz, K., Malan, D.J., Fulford-Jones, T.R.F., Nawoj, A., Clavel, A., Shnayder, V., Mainland, G., Welsh, M., Moulton, S. (2004) 'Sensor networks for emergency response: challenges and opportunities', *IEEE Journal on Pervasive Computing*, Vol. 3, No. 4, pp.16–23.

Maji, A.K., Mukhoty, A., Majumdar, A.K., Mukhopadhyay, Shamik Sural, Paul, S. and Majumdar, B. (2008) 'Security Analysis and Implementation of web-based telemedicine services with a four-tier-architecture', Paper presented at the *2nd International Conference on Pervasive Computing Technologies for Healthcare* (*PervasiveHealth 2008*), January 30–February 1, Tampere, Finland.

Medlin, D.B., Cazier, J.A. and Foulk, D.P. (2008) 'Analyzing the vulnerability of U.S. hospitals to social engineering attacks: how many of your employees would share their password?', *International Journal of Information Security and Privacy*, Vol. 2, No. 3, pp.71–83.

Mondy, J. and Torresi, M. (2008) 'CIGNA creating a virtual health care community', Cigna website, news releases. Available online at: http://newsroom.cigna.com/article_display.cfm?article_id=925 (accessed 20 June 2011).

Ng, H.S., Sim, M.L. and Tan, C.M. (2006) 'Security issues of wireless sensor networks in healthcare applications', *BT Technology Journal*, Vol. 24, No. 2, pp.138–144.

Samy, G.N., Ahmad, R. and Ismail, Z. (2010) 'Security threats categories in healthcare information systems', *Health Informatics Journal*, Vol. 16, No. 3, pp.201–209.

Schopp, L.H., Hales, J.W., Quetsch, J.L., Hauan, M.J. and Brown, G.D. (2004) 'Design of a peer-to-peer telerehabilitation model', *Telemedicine Journal and E-Health*, Vol. 10, No. 2, pp.243–251.

Stanberry, B. (1998) 'The legal and ethical aspects of telemedicine. Data protection, security and European law', *Journal of Telemedicine and Telecare*, Vol. 4, No. 1, pp.18–24.

U.S. Congress (2004) *Health Insurance Portability and Accountability Act* (H. REPT. 104-736), Government Printing Office, Washington, DC.

Varlamis, I. and Apostolakis, I. (2010) 'Self-supportive virtual communities', *International Journal on Web Based Communities*, Vol. 6, No. 1, pp.43–61.

Wozak, F., Schabetsberger, T. and Ammenwerth, E (2007) 'End-to-end security in telemedical networks – a practical guideline', *International Journal on Medical Informatics*, Vol. 76, Nos. 5/6, pp.484–490.

Notes

[1] Second Life Website: http://secondlife.com/

[2] Health Information Trust Alliance website: https://www.hitrustcentral.net/

[3] COBIT Framework for IT Governance and Control website: http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx

[4] According to EU Data Protection Directive (95/46/EC) (Article 2d), 'data controller' 'shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data'.

[5] In Annex A of ISO 27799:2008 the action of user A is theft by insider (threat number 21) and the action of users B and C is theft by outsider (threat number 22).

[6] In Annex A of ISO 27799:2008, such an attack is categorized as masquerading by outsiders (threat number 3).

[7] In Annex A of ISO 27799:2008, this type of threat is categorized as introduction of damaging or disruptive software (threat number 5).

[8] DataLoss database report of incident 1935. Refer http://datalossdb.org/incidents/1935-laptop-containing-the-personal-details-of-about-200-cancer-patients-stolen

[9] Lucile Packard Children's Hospital Appeals CDPH Fine (September 2010). Refer http://www.fiercehealthcare.com/press-releases/lucile-packard-childrens-hospital-appeals-cdph-fine

[10] London Hospital back online after computer virus shutdown (November 2008). Refer http://www.theregister.co.uk/2008/11/21/barts_mytob_recovery/

[11] Ponemon Institute's Benchmark study on Patient Privacy and Data Security. Sponsored by ID Experts. Refer: http://www2.idexpertscorp.com/resources/healthcare/healthcare-articles-whitepapers/ponemon-benchmarkstudy-on-patient-privacy-and-data-security

[12] A recent vulnerability that has not been identified and patched and has already been exploited by attackers.