# A holistic perspective of security in Health related Virtual Communities

I. Apostolakis[1], A. Chryssanthou[2], I. Varlamis[3]

[1]Visiting Professor,
Dept. of Health Economics,
National School of Public Health,
Greece
gapostolakis@nsph.gr

[2]Coca Cola Hellenic Bottle and Company,
Athens, Greece
argiris79@yahoo.com

[3] Visiting Lecturer,
Department of Computer Science and Technology
University of Peloponnese,
Tripoli, Greece
varlamis@uop.gr

## Abstract

A significant issue in health related applications is protecting a patient’s profile data from unauthorized access. In the case of telemedicine systems a patient’s medical profile and other medical information is transferred over the network from the examination lab to the doctor's office in order for the doctor to be able to perform a diagnosis. The medical information transferred across the network should be encrypted, secured and protected until it reaches its final destination. Patients' medical profiles should be accessible by their doctors in order to support diagnosis and care, but must also be protected from other patients, medical companies and others who are not certified by the patient to access his medical data. A very important element of virtual communities is trust. Trust should be built upon the same specifications for secure data transfer and leveled access with medical information. Furthermore, trust requires a strict policy based mechanism, which defines roles, access rights and limitation among community members, as well as a flexible identification mechanism, which allows anonymity of patients, while in the same time guarantees the truthfulness of doctors' identity and expertise.

## *INTRODUCTION*

The web offers access to many databases that contain medical information, and has significantly changed the way patients seek medical help. According to recent surveys, 50% of patients access medical information via the internet before visiting their doctor and this information affects their choice of treatment (Ferguson, 2002). The assistant role of virtual communities for patients who seek for medical help and advice is undeniable. Researchers, practitioners, medical industry and patients jointly contribute their findings, products and experiences, to the community's knowledge base. The information transferred inside a health related virtual community and the stockpiled knowledge must be carefully protected from unauthorized use and validated in order to be qualitative and useful.

The issues of security, which traditionally applies to telecommunication applications, and confidentiality, which applies to healthcare applications, smoothly converge towards trust, which is the basis and apex of communities (Mezgar, 2005). This chapter examines various aspects of a health related virtual community always under the prism of information security and user protection. We provide several paradigms where patient information may be at risk and others where the integrity of the exchanged information can be questionable due to security faults.

The following section provides an introduction to the main community concepts and defines the structure of a typical health related virtual community. The critical features of communities (aim, limits, roles, services) are examined in the scope of a health related community. The third section deals with health information in general and with the security issues, which might arise when using medical services from distance. In the third section, we argue for the need to protect medical data on access, in transit and in storage, we summarize the possible security risks and state the need for an integrated security management system. The last section, uses an fictitious example in order to demonstrate the use of security policies, which can be help virtual communities to protect knowledge and information sharing and guarantee integrity.

Our objective in writing this chapter is:

- to enlighten the public in the security and integrity issues inside community,
- to raise the level of security awareness: a) of IT professionals, who develop, maintain or contribute to health related communities, b) of patients that reveal their privacy to a "virtual doctor" and make use of medical advices shared by other community members,
- to propose a set of technologies, which can under circumstances ensure that patients and doctors benefit from using community services without the fear of being a pray for phishers, spammers, hackers and crackers,
- to define the steps for building a trustful health related virtual community.

## *HEALTH RELATED VIRTUAL COMMUNITIES*

This section provides a short introduction to the role of virtual communities in healthcare giving emphasis to the community structure and presenting the critical features of a healthcare community (aim, limits, roles, services). The section concludes with issues such as confidentiality and integrity of the community services and content.

In the process of psychological and medical support of patients with special needs three different types of participants can be distinguished: care providers, care givers and patients (Varlamis & Apostolakis 2007): *Care providers* are healthcare professionals, doctors and nurses, who treat and support patients as part of their work. The group is extended with researchers and scientists that convey their expertise on diseases and potential medical treatments. *Care givers* are those people who help a patient as friends or family of the patient. The group is extended with people who help voluntarily or otherwise deal with a specific disease, such as cancer. *Patients* are the "receivers" of the support. Care providers should be constantly informed on the scientific and industrial advances, on new products, treatments and devices. Researchers and scientists should disseminate their findings and guide industry and practitioners in favour of patients. Care givers should exchange information and useful hints concerning patients' care and support. Patients' needs vary over time, in the course of their disease experience: they want information in the first phase, when they learn about their disease and treatment alternatives; later, they are more interested in compassion and request emotional support (Varlamis & Apostolakis 2006). The BCANS community site (http://bca.ns.ca/) is a perfect example of patients and medical staff working in harmony by the means of a virtual medical community to fight the monster as they call it, namely breast cancer. They are performing that in a status quo of:

a) Deep trust, where users share trusting interpersonal relationships built on liking and mutual appreciation between people that have to work together on a mutual goal.

Or

b) Thick trust, where users trust each other based on personal experience or up-to-date info about a person's trustworthiness

Or

c) Swift (scatter) trust, where users trust each other based on some background of shared social network

(Patricia Radin, 2006)

**Tasks and roles**

One of the most important tasks in a virtual community is the coordination of discussion groups, which is handled by the group moderators (Moon, 2005). An important task which contributes to the building of trust inside the community is the administration of user profiles. The profile moderators check members' credentials and guarantee the truthfulness of their profile. This is possible through mini self-biographies. New users, who are "lurking" in the community's forums, need to feel comfortable enough, in order to participate in the community by talking about their problems, offering compassion or participating in group activities. Administrators protect the community from fraud and guide new members to the appropriate discussion and support groups based on their individual profiles. They guarantee the patients identity, distinguish care givers from medical professionals and in the same time protect patients' privacy by assigning them a virtual identity. In order to guarantee the quality of information provided to the community members, an additional moderator role is necessary: the content moderator, who is made responsible for reviewing and filtering all published material and acts as a liaison between information providers (experts, doctors, etc) and consumers (patients).

The aim of restricting access to the community only to members, is to build a status quo of thick trust among members and to protect them from outsiders (i.e. spammers, who advertise products, or ***phishers***, who gather and exploit personal data of members).

The different roles and tasks carried by each type of community's users are displayed in Figure 1. In the same figure the two valuable community sources; the Knowledge and Profile base offer multilevel access to members according to their role. Only registered community members are able to communicate and collaborate.

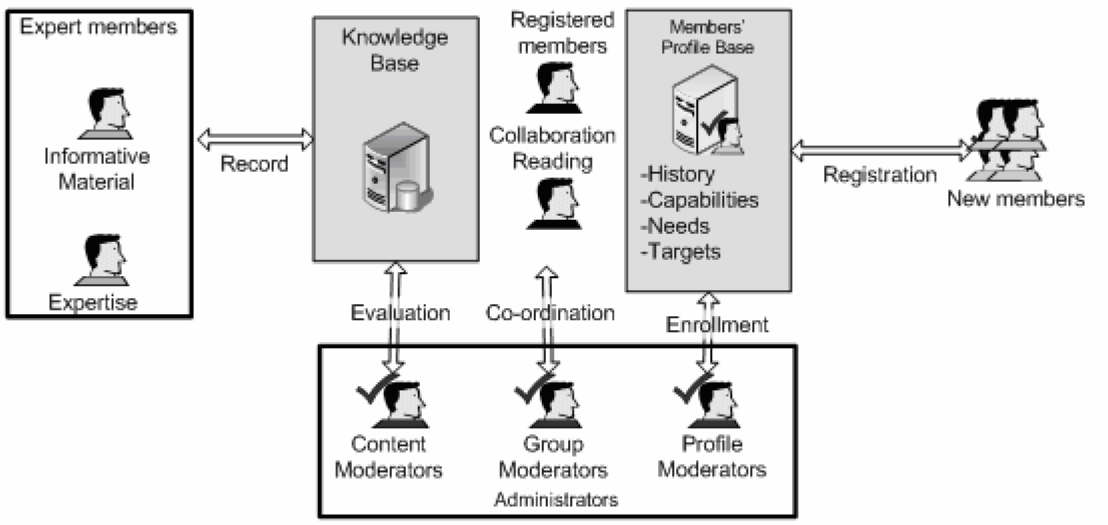

**Figure 1 Community roles and responsibilities**

We consider health related virtual communities as a large-scale distributed system, which offers services and allows transfer and storage of data. An important issue for the designers of a community is the building of trust among members. This requires that the administrators are aware of the complete profile of a member, whilst all other members have partial access. The protection of members' *anonymity* (Tygar, 1998) is crucial in a community of support and can be attained through the virtual identity of members. Virtual identity is always bound to the same user and stands for the static profile, thus allowing doctors to keep a history of their patients, while at the same time, preserves personal data of patients.

## Secure use of services

The services provided to the members of a supportive community must be carefully designed in order to be as useful to patients as possible. Extra care should be taken to guarantee accessibility of content and services and to avoid member exclusion. A patient joins a virtual community in order to obtain medical advice and care by doctors or support by fellow people, or co-patients. It is crucial for the patient to be able to access the community's services and content 24 hours a day 7 days a week. Consequently, computer security measures, such as the ones that will be analyzed later in this chapter, are necessary to ensure constant availability of the virtual community. Furthermore, appropriate access control mechanisms need to be in place to allow authorized users, namely the members of the virtual community, to enter the community site and benefit from its services, while blocking any unauthorized individuals from being able to enter the site with malicious intent. Access controls, such as security tokens, will be discussed further in this chapter. Data stored in the medical community's site should be regularly backed up offsite, so that they can be recovered safely in case of a disastrous incident.

The most widely used service is the distribution of ***informative content*** (i.e. medical documents, surveys, medical advices, news etc.). Content should be easily located and retrieved from patients. This subsumes that content should be available in various formats, so that it can be accessible to people with disabilities (deaf, blind etc). In order to facilitate new users, content can be forwarded to patients via e-mail through the appropriate mailing lists. For frequent users, content can also be published through a web portal. It should be organized into meaningful categories and a search service should allow retrieval of the appropriate information.

***Information dissemination*** through the website of the virtual community or by means of mailing lists requires security measures to be taken in order to ensure the safe transfer of medical data. In the first case (website transmission) cryptographic protocols, such as ***SSL (Secure Socket Layer)***, can be used by a member to communicate with the community site. Provided that the users use an e-token to enter the site, as suggested later in the chapter, the encryption process is handled entirely by the token, which requests from the server to "speak" a common cryptographic algorithm during their communication. Therefore, the patients need simply to enter a password for the e-token to communicate securely. The ***E-token USB device*** encrypts the whole communication between the end-user (member of the virtual community) to the virtual community's web server with a 256-bit security key.

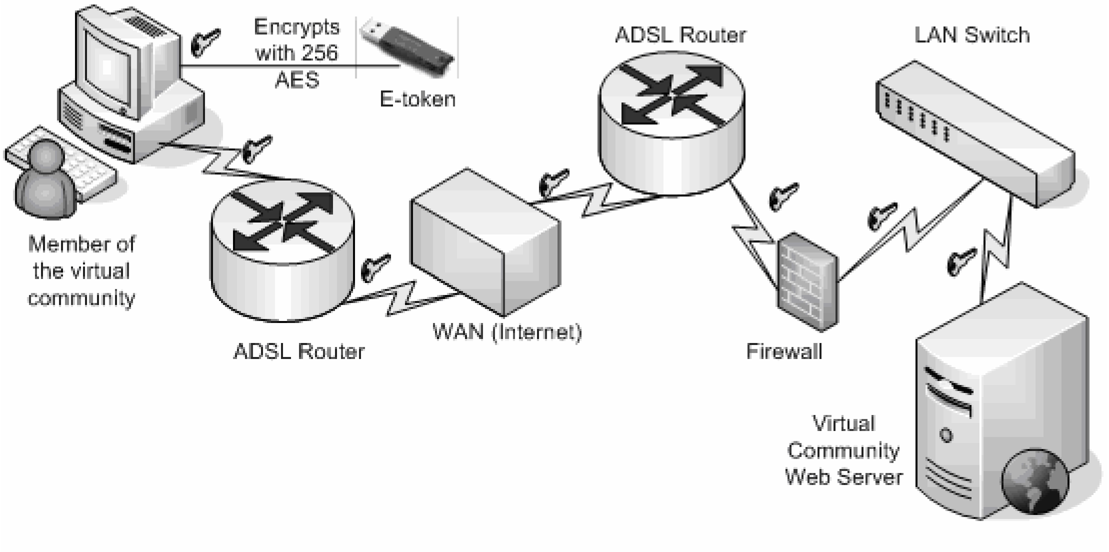

**Figure 2 - Secure Communication by means of an e-token usb device.**

An alternative could be the use of Virtual Private Network technology as an access control measure. A ***Virtual Private Network*** (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. Since the users of the virtual community enter the community site by means of an encrypted tunnel any conducted communication is private therefore secure.

In the case of ***e-mail communication, public-key cryptography*** should be used to ensure that mail communication can be read only by the intended recipient. In public key cryptography both communicating parties have a pair of keys, a public and private key. If a fictitious character named Bob wants to send a message to a person named Alice by using public-key algorithms, he just has to obtain Alice’s public key and encrypt his message with it. After encrypting the message the only person capable of decrypting the message is the one holding the private key, thus only Alice can decrypt the encrypted message and read it.

Interaction between community members is increased with online and offline discussions (Rada, 2005). ***Discussions*** can be asynchronous (by posting questions and answers) or synchronous (in a discussion ***forum*** or in private chat-rooms). The aim of discussions is bi-fold: to support patients and their families and to allow experts to exchange knowledge. Debates are more meaningful, when their topics are predefined and organized. The discussions in the community forums should be moderated by expert users that filter information when requested, facilitate members or consult members about the forum rules. The presence of professionals (doctors, nurses etc) in a forum adds to its value and increases participation.

Additional services allow members to provide information about themselves to the community and build their profile. The part of the ***user profile***, which is provided by the user himself, is his static profile and remains unchanged. Both patient and doctors should be able to update their member profile so that the community knows their current interest or expertise. Another part of the profile, which evolves all the time, is the dynamic profile which encompasses all actions of a member inside the community. In order to increase member interaction with the community and exploit the expertise of members, moderator roles could be assigned to frequent members, who will be requested to submit their feedback on the community operations.

Finally, in an autonomous community members should be able to make their own, ***self-supportive groups*** inside the community. Members of a group should be able to set-up or attend chat sessions on topics of interest, to participate in point-in-time surveys or straw polls on a topic to allow communities to gather consensus and determine community activity, to start new communities related to specific problems and steer the content according to their collective needs. The security measures mentioned above (encryption, tokens) apply naturally to all types of information exchange between members of the virtual community.

## *COMMUNITY'S VITAL ISSUES*

***Trust*** inside a community is built upon regular, honest, and cooperative behaviour (Fukuyama, 1995). In the case of a health related community, the ***person oriented dimension*** of trust is first built between the doctor and his patient and second among patients. In order to support trust between doctor and patients, the doctor's identity should be valid and accessible to the patient and on the other side, the patient’s profile should be made available to the doctor.

The other two dimensions of trust, as stated by (Fogg & Tseng, 1999), more specifically the ***trust in the object*** (such as computers, networks, and software) and ***process*** (such as tele-healthcare, or tele-consultation) can be met but more slowly. Although, many technological issues have been solved, the building of trust towards networks, security mechanisms and other technology issues is difficult. The build of trust towards the process can be facilitated with the definition and implementation of access policies to the medical information and services. A presentation of the approaches that capitalize on the building of trust in a health related virtual community follows.

### *Threats for the virtual medical community*

Threats that might damage the virtual community and cause the circulation in public of important medical data are among others:

i. Unauthorized access: A malicious user manages to infiltrate the community site and gains access to all these data that the community needs to protect.
ii. DOS (Denial of Service) Attacks: Malicious users use a number of computers to flood the community site with messages and take down the site and impair service availability.
iii. Identity theft: Someone manages to enter the community with a stolen identity. In such case, the malicious user might pose as a doctor and provide a patient with erroneous advices.
iv. Unauthorized copying of medical data: A user manages to copy the medical data of a patient and sell it along with a patient's identity to an interested third party.
v. Eavesdropping: A malicious user is spying information exchanged between community members and collects useful information.

The above mentioned threats could come from internal users (patients, the doctors and the moderators) as well as from external ones (McClure et al, 2003), such as:

i *Hackers:* skilled programmers, who attack information systems, aiming to achieve absolute knowledge of information technology

ii *Crackers:* skilled programmers, who attack information systems, aiming at personal gain either in financial or information level (information is power for the one who holds it)

iii Script-kiddies: good programmers, who employ hack tools in order to find exploits in the community platform and bring it down.

The potentiality of these threats depends on various factors:

i Main elements of the community infrastructure

ii Technical Vulnerabilities of the community systems

iii Handling of security issues by the members of the community

iv Value of the community's information for people outside looking in, such as crackers.

### *Securing the use of health services*

All members of a community -patients, their families, doctors, nurses and students of medicine- make use of the community services for their own reasons. Patients, for example, access the community in order to get the results of a medical examination or to obtain some medical advice, doctors in order to edit a patient's data or perform a diagnosis etc. Tele-medicine and tele-advice are two important services of health related communities, which both require the transfer of medical data.

Transfer of Medical data (examination results, medical information, medical advice etc.) obeys to the laws of CIA, where CIA stands for ***Confidentiality, Integrity*** and ***Availability***. Medical data is confidential, must be accurate and available during all times and is protected by Data Protection Laws. A process must be applied upon design and on launch and operation of the virtual community, which will guarantee that care providers, care givers and patients discuss in a secure manner. No user is eavesdropping, no one is collecting data (medical condition, mail address, financial data) for ***phishing*** or spamming purposes. This process must follow international standards such as BS7799 and ISO 27001, which define the lifecycle of an Information Security Management System.

A framework that has already been used in other medical information systems is the Octave Risk Management Framework. The framework consists of an organizational, a technology and a strategy and plan development phase. According to the framework a risk assessment identifies critical assets and potential threats in the first phase. In the second phase, key components and technical vulnerabilities are identified. In the final phase mitigation plans and a protection strategy are designed.. The goal is to build a security “stronghold” of information, where medical data and confidential discussions remain private, is not altered in any way and is constantly available.

### *Securing medical data*

In this section, we argue for the need to protect medical data on access, in transit and in storage. Technologies such as web sign-on, cryptographic algorithms, patch management suites and usage agreements are deemed necessary, so that all users, can use the community services securely (Chryssanthou & Kastania, 2006), (Chryssanthou, 2006).

Web sign-on can be used by members of a virtual community upon login on the virtual community site. By using this technology users can identify themselves correctly and communicate with each other by means of a cryptographic algorithm. ***Web sign-on*** is performed usually by using an ***e-token*** usb device which can be provided to the user upon registration. This e-token can store passwords in an encrypted state and when used encrypts the user’s communications with algorithms such as AES. ***Cryptographic*** algorithms ensure confidentiality of communication. Any eavesdropper will “hear” cryptographic gilberish. Depending on the quality of the used algorithm the potential eavesdropper might never get any useful data from “hearing” a user’s conversation.

Computer systems are vulnerable to problems of the operating system and have several security holes. Most of these vulnerabilities are discovered also by members of the hacking community. Manufacturers update their software, in order to keep up with the “bad” hackers and ensure that their customer’s data remain secure, but unfortunately they cannot avoid zero-day exploits. Zero-day exploits are exploits that are deployed on the net before a manufacturer has the time to provide a fix for a particular vulnerability. To tackle with zero-day exploits a further security component such as an ***Intrusion Prevention System*** is needed. This type of system will be able to block any suspicious traffic based on the characteristics of the received data.

The members of a virtual community discuss about sensitive medical issues, handle medical data and might disclose very sensitive private information, which would prove to be a goldmine in the hands of a skilful hacker, a spammer or a phisher. Thus, the members of the virtual community do not just need to feel protected against potential threats, they also need to be aware that even in a case of a breach the appropriate measures are in place, which will ensure that the potential perpetrator is found, before their data turn into a valuable asset for the highest bidder in the pharmaceutical community. The logs, which are maintained by an Intrusion Prevention System, will certainly play an important role in finding a potential perpetrator. A well justified and designed procedure that will guide the moderators in performing a ***forensic analysis*** of a potential incident, while recovering through a backup plan in the minimum amount of time, will be another important aspect of these measures. Forensic analysis (Chryssanthou & Apostolakis, 2006) is the procedure, during which the appropriate personnel, either internal or external, images hard disks, collects network traffic logs, system logs, hashes the evidentiary data, so that it can be used in a court of law. This vast amount of data is collected and analyzed by using special tools (i.e. Encase from Guidance Software and The Forensic Toolkit by AccessData, Helix and F.I.R.E).

It might also prove useful to set up a honeypot to draw back the perpetrator in order to trace him back to his location, collect data on the type of his illegal activity or just collect data that will help reveal the perpetrator’s true identity. In computer terminology, a honeypot is defined a trap, which seems to contain information that would be of value to attackers, and which is set to detect or deflect attempts at unauthorized use of information systems.

***Backup systems*** are also necessary so that the systems can return to a previous known state without the users losing their data and with the minimum cost in availability. A medical site should remain offline the least amount of time, because time is of great importance in all medical cases.

***Usage agreements*** are not a technological security measure, but still play an important role in a network security infrastructure, especially in a web community. They are written based on the results of the risk management process and according to the data protection laws governing medical data. Users have to know how the virtual community operates, what its purpose is, what is allowed and what prohibited and which legal consequences might arise on violation of the usage agreement.

### *Building trust inside the community*

In this section we focus on the necessary security policies, which can be implemented in health virtual communities in order to protect community members from improper use of services, deception and other possible hazards inside the community. This section crosses the technical barriers of information security and data privacy and presents a holistic perspective of security inside a community. This perspective examines people, processes, strategies and community culture.

A fundamental requirement for a successful community is to build trust among the community members and consequently enforce members' confidence to the community mechanisms. A community is trusted when it implements a security policy mechanism. The first action of community designers is to define the appropriate policies, to describe the roles inside the community, the access rights and restrictions for each role etc. The design of the community should follow the security guidelines: provision should be made for user roles and credentials and an access control mechanism should be implemented over information and services. This would be made possible by using access policy models. A prototype access policy for a medical community is the Cassandra trust management system for electronic health records (Becker & Sewell, 2005). Cassandra is a role-based access system (RBAC) expressed on a language based on Datalog with constraints. Access control is based on the member's role in the community. Furthermore, the data owner can define the sensitivity of his data, the people able to access it and the access rights, by which each allowed user can access his data.

For example, a treating physician can access a patient's entire medical file, while a receptionist can only view and alter (with the patient's authorization) his general data. Credentials can be distributed by registration authorities or by patients. For example, suppose that a patient needs to undergo a surgical operation. The patient grants the treating doctor access to his medical doctor to access his data in order to perform the surgery. The doctor can now give access to his data to the other members of the medical team so that they can assist during surgery. The roles assigned to the members of the surgical team (Register-team-episode) are valid only for a period of time (during surgery and for treatment. Upon recovery of the patient the roles are revoked. In a virtual medical community a similar semantic role-based policy has to be applied. The general roles (patient, doctor, advisor, etc) can be assigned by the moderators. Patients then can define which doctors can access their private data or which members can take part in a private held conversation. This access policy will be enforced by each user upon entering the site of the virtual community. On first registration, the users will have general access rights based on their type of user (doctor, patient, etc).

The access policy is supplementary to the access control mechanisms mentioned earlier. An access control policy will be implemented technically, explained to the user on registration and will be available as a written and electronic document so that the users have no excuse for violating other user's rights or the policy in general and the community is protected against users' misbehavior. This written document will explain everything, from login procedures, password quality, privacy rights to user roles and credentials.

In a health related community, the problem of trust is multifold: patients should be confident that their doctor (or medical consultant in general) is capable to support them, they should be sure that the communication with their doctor is sheltered from unauthorized access and that their doctor is discreet with their problem. The patients have to be certain beyond any reasonable doubt that they are talking to a doctor and not an impostor and that their conversation with a doctor is held in private (protected by doctor – patient confidentiality). In several cases, it is desirable for patients to hide their identity even from the doctor, thus allowing them to express their problems or worries more sincerely. On the other side, doctors share their expertise with the patients, and request access to patients' health profile in order to provide better diagnosis and support.

Inside a virtual community, patients and doctors are hidden behind their virtual identities. A user is anonymous without obtaining the right not to be liable for any disrespect or violation of the community's regulations. A difference between health related communities and other community applications is that the history of visits as well as the role of a member inside the community is of importance to other members. For example, patients, who engage on a discussion with a doctor, want to be absolutely certain that their interlocutor is a real doctor. Furthermore, they need to be aware of his/hers field of expertise. Similarly, doctors need to access the complete patient's profile and medical history before making their diagnosis. Doctors will be allowed to access the complete patient's profile only after obtaining the patient's consent by the means of a role assignment (for example treating physician role) through a properly formed semantic policy.

It is clear from the above that the virtual identities of all community members should remain unchanged throughout their "virtual life" in order to allow the creation of dynamic profiles and facilitate doctors' work. Parts of the real identity of doctors (i.e. their expertise) should accompany the virtual identity, in order that the users of the virtual community build a thick trust relationship. Enhancing the doctor's avatar with a short bio of his medical accomplishments will certainly convince the patients to open up about their problems, trust the doctor and obtain helpful medical advices.

### *User's Responsibility of Security*

All the security technologies, which were analyzed and proposed earlier in this chapter, focused on protecting and encrypting communications on the one side and controlling access to the main infrastructure on the other. However, a basic factor has been left aside: end users. Kevin Mitnick used to say that there is no cure for human stupidity. The strongest security mechanisms are of no use when a naïve user shares his/her password with an unknown person. Users need to be security aware, not give their passwords or their keys to anyone and should not just hang on the security measures handed to them by the community. A fully updated antivirus product on their own personal computer can protect them from ***keyloggers***, namely programs that will try to log their keystrokes, ***Trojans***, programs that do not perform just as intended, ***spyware*** and of course viruses. What's the point of building a secure channel if the one end of the connecting line is not secure? Both ends of a communication line need and must be secure in order for any security mechanisms to have a real effect.

### *Combining the strengths of BS7799 and ISO 27001*

As a conclusion, in order to achieve international security standards during designing and implementing the community, an Information Security Management System has to be designed. The international standards in the computer security area are the BS 7799 (BSI, 2005) and the ISO 27001(IEC, 2005) (IEC$_2$, 2005). Both standards define the right way to implement an effective Information Security Management System. Building such a system is a result of a continuous cycle of procedures, which repeats itself as the needs of an organization change, the legal regulations change and security regulations evolve, while their "opponents", the tools, that the perpetrators of e-crime use, become more and more sophisticated. This cycle consists of 4 stages, namely: *Plan, Do, Check* and *Act* as depicted in Figure 3.

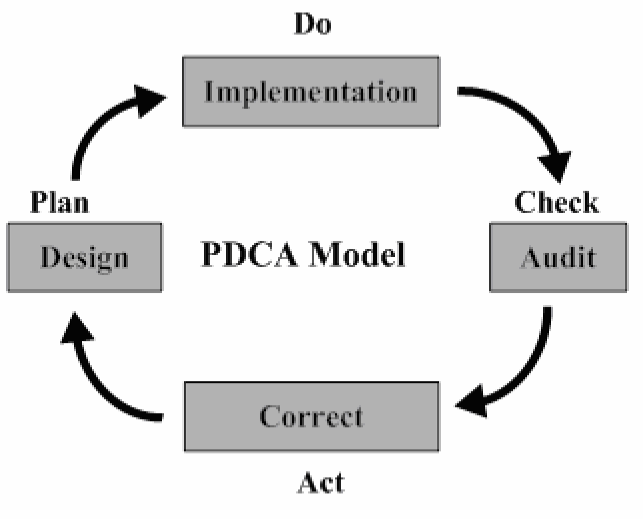

**Figure 3: The Information Security Management cycle**

An Information Security Management System, in essence, is a “live” part of an organization, which has to be designed correctly (based on various parameters), implemented based on technologies, that are selected during the design phase and checked for its effectiveness. This check will result in identifying possible changes, which are necessary, in order for the system to improve or to adapt to new circumstances, such as a new stricter computer law act. If such a system is surpassed by technological developments then it stops being effective and the organization, which uses it, is in immediate danger of computer security breaches.

## A VIRTUAL MEDICAL COMMUNITY SCENARIO

In order to achieve our objective a fictitious health related virtual community will be used as a paradigm. This community must be evaluated from a security perspective by the means of globally accepted security standards such as BS7799 and ISO27001. The community structure, the appropriate trust building mechanisms and policies will be discussed in the following.

If we abstract the interaction between a doctor and a patient inside a virtual community to a transaction between two people in which one requests assistance and the other offers it we can easier discover the critical security issues. In the following we describe a community comprising patients of a group therapy program and the affiliated doctors and this is our exemplar case study.

Both patients and doctors access the community web server using their browsers. Patient's real identity must remain hidden to all community members, and only the community administrators should be able to access it. This type of anonymity is crucial for a group therapy community to attract potential members.

In order to support this partial anonymity we need a flexible patient profile, which contains both identity and medical information, and which has access control policies.

When patients and doctors log into the community, they apply the appropriate credentials and get a virtual id, which remains constant throughout their virtual life.

This virtual identity offers anonymity while in the same time guarantees atomicity. Patients are identified as patients and their virtual profile is enhanced each time they join the community: the group therapy sessions in which they participate are recorded in their dynamic profile (history) and the same holds for their activities. This information is available for doctors who monitor patients’ behavior. Doctors are identified in a similar way and their field of expertise appears in their publicly available profile. The identification of doctors and patients increases the confidence of patients to the community experts (psychologists, pathologists etc) and makes them more positive in participating to virtual group meetings or private sessions. The virtual identity conceals the real identity from unauthorized view and increases patients' openness in discussions.

Upon identification, patients gain access to their own space in the community server. There, they are able to update their personal and medical profile information. Patient's medical profile is valuable for the doctor but is of no use to the other patients and as such it must remain out of their access. The patient must be able to define which user groups or specific users should have access to their profile information (e.g. my doctor, my friends, user X etc) and to which specific part of it (i.e. medical information, personal information etc)

After updating her profile, the patient is able to contact a doctor and discuss her problem. The patient grants access to the medical profile to the doctor at any time. The doctor uploads a diagnosis and consultation and grants access to the patient (or to an accredited member of his family). No other doctor is able to access this medical profile unless the patient gives a grant option to the doctor. Similarly, the diagnosis is accessible to the patient only. The same holds with any examination results.

***Define sensitive data***

The first important asset of a medical community, whether virtual or not, is medical data. Medical data is twofold. It consists of the identity of the patient and its medical file. Having one without the other or being able to identify the other is useless for financial purposes. Having both provides a repository of information, which can be of value to patients, doctors, insurance, pharmaceutical companies and medical organizations. This type of data is sensitive and protected by international computer laws such as the EU 95/46/EC directive (EU, 1995) and national laws such as law no 2472 for the protection of an individual against unlawful processing of personal data (Greek Data Protection Authority, 1997). Medical data abide to the laws of CIA and need to be protected so that cases like the one of Privacy Rights Clearinghouse (PRC) v. Albertsons, where a chain of pharmacies was collecting data about their customers, which were used for illegal marketing of pharmaceutical products, are not repeated. (PrivacyRights.org, 2004) Such a case is clearly illegal in the EU, as this chain of pharmacies violated contract laws, connected medical files without authorized permission, violated the confidentiality of medical data and engaged in illegal marketing. Consequently, a virtual community must remain a virtual community; ***medical data*** must be protected ***in whatever form they are uploaded*** in the community, ***medical conversations*** must remain confidential and ***virtual identities*** must never by any means be identified with a patient’s or a doctor’s real identity. Medical data, medical conversations and virtual identities are the most important information assets of a virtual medical community, assets which must be identified by the designer of the ISMS in the design phase while performing risk analysis.

### *Defining hazards*

The first phase of the risk analysis was to identify the most important information assets, which need to be always protected. The second phase would be to identify what these assets need to be protected from and the potentiality of those threats. The hazards for the healthcare community comprise unauthorized access to data and services, attacks, data and credentials stealing, eavesdropping and have been detailed in the previous. The biggest threat for a healthcare community is eavesdropping because it is difficult to be detected and refers to sensitive personal data. DOS attacks are less likely in a healthcare virtual community. Other threats can be minimized by choosing and implementing appropriate security and identification mechanisms.

### *Choosing the technologies*

First of all, the community must be shielded against unauthorised copying. For this reason, a written policy will be sent to the users and must be agreed on during registration. This written policy will define security procedures, emphasize on the sensitivity of the exchanged data, and inform the users of the legal consequences of unauthorized copying or publishing of community's data as well as the consequences of damaging in any way the community's infrastructure. This written policy must be supplemented by an actual technically implemented policy which will assign specific rights to the users on first entry.

The access policy will be role-based and will follow the semantics model proposed earlier, in order to allow patients to assign different rights to their treating doctor than other doctors, who simply will need to see a portion of the data to provide them with an advice. Simultaneously, a doctor will be able to add hidden comments about a patient's medical condition without the patient knowing about it. Access to the repository of real identity information will be restricted only to the administrators group, will be allowed only when at least two administrators agree and any access will be audited. Auditing, of course, will be enabled for all access to sensitive data.

A second measure is to ensure that no one is eavesdropping. In order to achieve that all communications will be encrypted. Encryption is bi-fold: first, the web server has to speak a cryptographic "language" such as SSL and second, the user's browser has to speak the same "language". The encryption algorithm has to be as strong as possible. Upon verification of a user's data and completion of the registration procedure, a web sign-on e-token will be given to the user. The token will have a strong password and will comprise the community password. The only way to enter the community will be by using this token, which will encrypt the user's traffic. In this way, the possibility of identity theft and unauthorized access will be also reduced, as a malicious user would have to obtain a valid e-token in order to enter the community's site.

A third measure is to protect both ends of the communication. Users must install an antivirus in order to ensure that they are virus free and Trojan free. The infrastructure of the community must also be protected by a fully updated antivirus system and up-to date patched against technical vulnerabilities by means of a patch management suite. Furthermore an Intrusion Prevention System has to be in place with constantly updated signatures, in order to deal with hack attempts and DOS attacks.

The final step is to define a backup and recovery procedure. The community's data have to be backed up regularly so that the community can recover from a security breach or another form of damage. Backups should be kept in remote sites, while a recovery procedure has to be in place that will help regain functionality in the minimum amount of time in all possible scenarios.

These proposed solutions should be enough to protect a fictitious medical community against most important types of attacks. It hangs on the moderators and the support team to maintain security and achieve it. Security is a constant battle. Technologies change and attacks evolve, so measures must constantly be improved, while users must be always security aware.

## *Conclusions*

This chapter presented a holistic approach in securing transaction inside a health related virtual community and building trust among members and trust to the community mechanisms. The major requirements of this approach are: technical solutions that secure transfer of medical information (such as encryption etc), identification mechanisms that guarantee atomicity and allow anonymity per case and security policies, which grant access to medical information only to the appropriate community members. The necessary technology infrastructure exists, however it must be adapted to the specific community needs.

### References

1. Anargiros Chryssanthou, Ioannis Apostolakis, (2006) "Network Forensics: Problems and Solutions", in proceedings of the 2nd National Conference with International Participation, Electronic Democracy, Athens, ACCI.
2. Anargiros Chryssanthou, Anastasia Kastania, (2006) "Quality & Security in medical information systems", Health Review, Tome 17, Issue 100, pages 42-45
3. Anargiros Chryssanthou, (2006) "Security of Information Systems in Health environments", 6th National Conference on Public Health & Medical Services.Athens.
4. Anargiros Chryssanthou, (2006) "Gathering of digital evidence in a computer network : Problems & possible solutions", School of officers in research and informatics – Informational leaflet in Informatics & Technology, Issue 28, May 2006.
5. Tom Ferguson, (2002). "From patients to end-users". British Medical Journal, 324, 555-556
6. B.J. Fogg, Hsiang Tseng, (1999). "The elements of computer credibility", in the proceedings of CHI'99, Pittsburgh, PA.
7. Francis Fukuyama, (1995). "Trust—The social virtues and the creation of prosperity". New York: The Free Press.
8. Ivan Mezgar, (2005) "Building trust in virtual communities", Encyclopedia of Virtual Communities and Technologies. Edited By: Subhasish Dasgupta, George Washington University, USA.

9. Stuart McClure, Joel Scambray, George Kurtz. (2003). "Hacking Exposed, Network Security Secrets and Solutions", McGraw Hill Osborn, pp 408 -412

10. Jane Moon, (2005). "Discussing health issues on the Internet", Encyclopedia of Virtual Communities and Technologies. Edited By: Subhasish Dasgupta, George Washington University, USA.

11. Moritz Y. Becker, Peter Sewell. (2005) "Cassandra: Flexible Trust Management Applied to Electronic Health Records". Published as Technical Report UCAM-CL-TR 648, University of Cambridge, Computer Laboratory, pp 214

12. Roy Rada, (2005) "Cancer Patient-Patient Online Discussion Groups", Encyclopedia of Virtual Communities and Technologies. Edited By: Subhasish Dasgupta, George Washington University, USA.

13. Patricia Radin. (2006) "To me, it's my life'': Medical communication, trust, and activism in cyberspace. Social science and Medicine, vol. 62, pp. 591-601.

14. Doug Tygar, (1998) "Atomicity versus Anonymity: Distributed Transactions for Electronic Commerce" Proceeding of 24 International Conference on Very Large Databases (VLDB), August 24-27, 1998, New York City

15. Iraklis Varlamis, Ioannis Apostolakis, (2007) "Self supportive web communities in the service of patients", in the proceedings of IADIS International Conference on Web Based Communities 2007, 18-20 February, Salamanca, Spain.

16. Iraklis Varlamis Ioannis Apostolakis, (2006) "Use of virtual communities for the welfare of groups with particular needs", in the proceedings of the 4th ICICTH International Conference on Information Communication Technologies in Health.

17. British Standards Institution, BSI (2005). "Information technology. Security techniques. Information security management systems. Requirements". British Standard / ISO/IEC / 18-Oct-2005/ ISBN: 0580467813.

18. International Electrotechnical Commission, IEC (2005). "Information technology - Security techniques - Code of practice for information security management". ISO/IEC/ 17799/ 01-Jun-2005.

19. International Electrotechnical Commission, $IEC_2$ (2005). "Information technology – Security Techniques – Information Security management systems – Requirements", ISO/IEC FDIS 27001:2005.

20. The European parliament and the council of the European Union. (1995) "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", Luxembourg. (Directive 95/46/EC)

21. Greek Data Protection authority. (1997) "Individuals protection against the processing of personal sensitive data". (Law 2472/1997)

**Key terms:**

*Healthcare Virtual Communities:* Virtual communities comprising members from the healthcare domain. Members join the community in order to discuss health related subject, give or receive medical advice and support etc.

*Trust*: The most important factor for a long-living community. Trust can be deep, thick and swift depending on the strength of relation between community members.

*Sensitive Personal Data*: Data referring to a person, which cannot be revealed to anybody. In a health related virtual community, such data may refer to a person's health situation, nutritional restrictions, history of examinations and surgeries etc.

*Eavesdropping*: A malicious user is spying information exchanged between community members and collects useful information.

*Unauthorized access*: A malicious user manages to infiltrate the community site and gains access to all these data that the community needs to protect.

*Confidentiality, Integrity and Availability*: Medical data is confidential, must be accurate and available during all times and is protected by Data Protection Laws.

*Intrusion Prevention System*: A system which is able to block any suspicious traffic based on the characteristics of the received data and guarantees authorized access to the community information and services

Ioannis Apostolakis was born in Chania of Crete and studied Mathematics in University of Athens. He holds an MSc in Informatics, Operational Research and in Administration in Educational Units, and a PhD in Health Informatics. He has been for several years Scientific Researcher in the Department of the Clinical Therapeutics in University of Athens. He had been teaching in University of Athens and in Polytechnic University of Crete. Today he teaches to the post-graduate program of the National School of Public Health and to Panteion University.

Anargyros Chryssanthou 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). He has written and presented several articles in national conferences, concerning various aspects of computer security, from network forensics to cryptography, security management and ISO implementations of Information Security Management Systems (ISMS). He is currently employed by Coca Cola Hellenic Bottle and Company as a Database Reporting Specialist.

Iraklis Varlamis is a post-doctoral researcher in the Computer Science Department of Athens University of Economics and Business. His research interests vary from data-mining and knowledge management to virtual communities and their applications. He has written and presented several articles in international conferences, concerning the design and implementation aspects of virtual communities.

For more information visit: http://wim.aueb.gr/iraklis