Technical Guidelines for Enhancing Privacy and Data Protection in Modern Electronic Medical Environments

Stefanos Gritzalis, Costas Lambrinoudakis, Dimitrios Lekkas, and Spyros Deftereos

Abstract—**Raising awareness and providing guidance to on-line data protection is undoubtedly a crucial issue worldwide. Equally important is the issue of applying privacy-related legislation in a coherent and coordinated way. Both these topics gain extra attention when referring to medical environments and, thus, to the protection of patients' privacy and medical data. Electronic medical transactions require the transmission of personal and medical information over insecure communication channels like the Internet. It is, therefore, a rather straightforward task to capture the electronic medical behavior of a patient, thus constructing "patient profiles," or reveal sensitive information related to a patient's medical history. The consequence is clearly a potential violation of the patient's privacy. We performed a risk analysis study for a Greek shared care environment for the treatment of patients suffering from beta-thalassemia, an empirically embedded scenario that is representative of many other electronic medical environments; we capitalized on its results to provide an assessment of the associated risks, focusing on the description of countermeasures, in the form of technical guidelines that can be employed in such medical environments for protecting the privacy of personal and medical information.**

Index Terms—**Data protection, EU directives 2002/58, 97/66, 95/46, privacy, security.**

I. INTRODUCTION

THE immense advances in the area of Information and Communication Technologies (ICT) have supported the transition from standalone centralized computer systems to open networks and distributed computing environments. Nowadays, most applications capitalize on the advantages and the flexibility emanating from the ability to interconnect different computing systems via local area networks and the Internet. The healthcare sector is an indicative example of an application area that can benefit a lot from the development of a Web-based infrastructure [1]. The main objectives of the ongoing research and development work in the area are:

- to increase the quality of healthcare services;
- to support new applications, such as telediagnosis, etc.;

S. Gritzalis and C. Lambrinoudakis are with the Information and Communication Systems Security Laboratory, Department of Information and Communication Systems Engineering, University of the Aegean, Samos GR-83200, Greece (e-mail: sgritz@aegean.gr; clam@aegean.gr).

D. Lekkas is with the Department of Product and Systems Design Engineering, University of the Aegean, Syros GR-84100, Greece (e-mail: dlek@aegean.gr).

S. Deftereos is with the First Department of Internal Medicine, University of Athens, Medical School, "Laiko Hospital," Athens GR-11527, Greece (e-mail: deftereo@otenet.gr).

- to increase information availability;
- to reduce costs.

However, the problem raised is that of security, especially as the privacy of communication through the Internet may be at stake in a number of ways. Online collection and processing of personal data forms a severe threat to privacy, being the main conservation of the public as far as the utilization of Internet-based services is concerned. This fact has been confirmed by a *Business Week* poll [2], which has provided evidence that the major user reservation in using the Internet is due to the lack of privacy rather than cost, difficulties in using a service, or undesirable marketing messages. The problem becomes much more intense in modern medical environments [3]–[7] and especially in shared care environments in which healthcare services are offered by multidisciplinary teams of healthcare professionals [8] who may be located in different, often distant, healthcare units.

Healthcare networks are designed and developed in accordance to common standards (e.g., standardized electronic patient records) linking general practitioners, hospitals, and social centers at a national and/or international level. The development of such networks has resulted in the increase of the amount of sensitive medical information being collected, stored, shared among different healthcare professionals, and transferred to different sites worldwide [9]. Furthermore, it is common for such environments to support *electronic medical transactions* (in the form of telemedicine services) between the patient and the healthcare organization and/or other health professionals. The vast majority of such electronic transactions are being offered through the Internet, even though the exchange of personal and/or medical information is a clear prerequisite. It is therefore evident that specific measures are required for ensuring that users can access and process personal data only if this is necessary for the tasks they are authorized to perform (*privacy principle of necessity of data processing*) and if the purpose of data processing is in line with the purpose for which the data was obtained (*privacy principle of purpose binding*) [10]. Moreover, much attention must be paid to the *privacy principle of transparency*, so that patients should know who has access to their data and for what purpose. Needless to say, the confidentiality and integrity of the information transmitted over the communication channels (including the Internet) should be adequately protected.

Consequently, additional technical, procedural, and organizational measures are necessary for fulfilling requirements like integrity, confidentiality, availability, and accountability of the information exchanged through a telecommunication network.

It is stressed that the terms *security* and *privacy*, which are often confused in the literature, are distinct and complementary [11]: A piece of information is secure when its content is protected, whereas it is private when the identity of its owner is protected. Several privacy-enhancing technologies have been employed for protecting privacy [12]. However, a long list of technical countermeasures and a secure infrastructure are not enough for ensuring the privacy of the information. For instance, even if the existence of an ultra-secure hospital information system is assumed, it may be the case that the hospital decides to disseminate personal and medical data of its patients, thus violating the privacy of those individuals. In information society, privacy is adopted as a fundamental right of the individual and is related to issues like: the type of the information collected, how and for what purpose is this information used, how is it protected, shared, rented, sold, or otherwise disseminated [3]–[7].

This paper is organized as follows. In Section II, we briefly outline the legislation concerning privacy. Section III provides an overview of a shared care environment that includes several distant healthcare units, involved in the treatment of patients suffering from beta-thalassemia. This is a real scenario implemented through a well-established distributed electronic environment in Greece that treats beta-thalassemia patients for more than five years. The risk analysis and management methodology, namely the CCTA Risk Analysis and Management Methodology (CRAMM) methodology, that has been utilized for assessing the security level of the aforementioned beta-thalassemia scenario, is presented in Section IV, while the results of the risk assessment are presented in Section V. Section VI provides, in the form of general technical guidelines for electronic medical systems, the security measures that each "actor category" should employ for protecting privacy in accordance with existing legislation, with special emphasis on the actor categories of *Clients* and *End Service Providers*. Finally, Section VII provides some concluding remarks.

II. PRIVACY AND LAW

Privacy, as a social and legal issue, has for a long time been the concern of social scientists, philosophers, lawyers, and physicians. The United Nations Declaration of Human Rights, the International Convenant on Civil and Political Rights [13], and many other national and international treaties have recognized privacy as a fundamental human right that must be protected in democratic societies. Two American lawyers, S. Warren and L. Brandeis, defined privacy as "the right to be alone" [14]. In general, the concept of privacy can be applied in three different aspects [15].

- *Territorial privacy:* the protection of the close physical area surrounding a person.
- *Privacy of the person:* the protection of a person against undue interference.
- *Informational privacy:* the control of whether and how personal data can be gathered, stored, processed, or selectively disseminated.

Several researchers have tried to provide alternative definitions for privacy, expressing the above-mentioned "control" of an individual in terms of: property, autonomy, and seclusion.

Privacy may be understood as *property* in the sense that a person may give away part of the control over her/his personal information in exchange for some benefit. Furthermore, it may be perceived as *autonomy* in the sense that each person is free to partially or fully authorize a third party to obtain, process, distribute, share, and use her/his personal information for a specific aim. Finally, privacy may be understood as *seclusion* in the sense that everyone has the right to remain undisturbed. This paper deals with informational privacy and assumes that privacy is the indefeasible right of an individual to control the ways in which personal information is obtained, processed, distributed, shared, and used by any other entity.

With the arrival of modern ICT systems, privacy is increasingly endangered. As rapid computerization brought fear of a surveillance society, some nations sought to protect individuals from the misuse of personal data. In the European Union, the Directive 95/46, "On the protection of individuals with regard to the processing of personal data and on the free movement of such data" [4], sets the prerequisites for data owners and processors for collecting, processing, and exchanging personal information. The U.S. government promotes the notion of "self regulation," a set of data protection rules applying to a plurality of market sectors, the content of which has been primarily determined by members of the specific trade sector.

Several interpretations of the 95/46 Directive emphasize the use of unified codes. The tasks of collecting and/or processing data for Internet users (i.e., e-mail address, Internet Protocol IP address etc.) fall into the provisions of the above directive. Furthermore, telecommunication services, as stipulated in the 97/66 and 2002/58 Directives [5], [7], are protected by the provisions for the secrecy of the telecommunications. Public authorities may be allowed to access secret information, thus compromising secrecy, only for specific reasons and under specific conditions and procedures provided by the domestic country's legal framework.

The European Internet Task Force recently published a report concerning on-line data protection. It is important to mention the four guidelines that have been recommended for all European countries:

- raising awareness of the Internet users;
- applying existing legislation in a coherent and coordinated way;
- developing and using privacy-compliant, privacy-friendly and privacy-enhancing technologies;
- building trusted mechanisms for control and feedback.

In addition, identifying the "adequacy" of the protection level offered by a destination country has become the most distinct debate with regard to transborder data flow. The European Union Directive 95/46 [4] and the Council of Europe Model Contract of 1992 [16] have adopted the term "adequate level of protection," while OECD guidelines state that transborder flows may be restricted in case no "equivalent" protection exists [4].

III. A SHARED CARE ENVIRONMENT SCENARIO

The care model that has been studied, as a representative one in terms of the electronic medical transactions supported, the actors involved, and the potential risks for the confidentiality

and integrity of medical and personal data, is that of beta-thalassemia [17], a chronic disease that requires both emergency interventions and life-long follow-up examinations. Beta-thalassemia is a hereditary disease, which results from a mutation in the genes that are responsible for the production of hemoglobin. The hemoglobin found in healthy persons is substituted by a nonfunctional protein, thus leading to severe anemia, the onset of which usually lies between the fourth and sixth month of life. Untreated severe beta-thalassemia is uniformly fatal in childhood. Life can only be prolonged by periodic blood transfusions. Unfortunately, transfusions overload patients with iron, which deposits on virtually all organs causing significant damage. Heart failure, due to iron deposition on the heart, diabetes mellitus, due to its deposition on the pancreas, and hepatic failure, due to its deposition on the liver are only a few of the possible complications. As a result, patients suffering from beta-thalassemia need to receive continuous chelation treatment in order to remove the excess of iron from their body, as well as periodic hematology, cardiology, endocrinology, and hepatology evaluations. The content of these evaluations ranges from simple laboratory tests, such as complete blood count or oral glucose tolerance test, to complicated laboratory and imaging studies, such as heart and liver magnetic resonance imaging (MRI) scans. Some of the procedures, such as heart MRI, are performed on an annual or biannual basis, but others, such as blood transfusions and chelation, are performed every two to three weeks.

Only rarely does a single healthcare unit offer all required services. Typically, different services are offered in different, often distant, units, each of which maintains a separate record for every patient. Individuals originating from rural areas or small urban centers often need to travel to the capital to gain access to specialized care items.

Fig. 1 provides a high-level picture of the *entities* involved in the beta-thalassemia shared care scenario that has been studied. It is a distributed environment consisting of a Hospital Information System, located at the beta-thalassemia unit of the Hospital of Korinthos, a cardiology unit specialized in beta-thalassemia, located at the Laikon Hospital in Athens, Greece and a cardiac ultrasound unit, located also in Athens, all sites being interconnected through the Internet.

Some indicative examples of *electronic medical transactions* that are supported by the specific shared care scenario, but also by other similar distributed electronic medical environments are:

- Communication of Electronic Healthcare Records
  — to patients;
  — between different, potentially distant, physicians involved in the patient care process (for example, between diabetologists, cardiologists, radiologists and ophthalmologists that participate in the follow-up care of patients);
  — between medical units and specialized laboratories (for example, between the transfusion units, which are mainly responsible for the care of thalassemic patients, and the MRI labs in which the latter are measuring their heart iron-load).
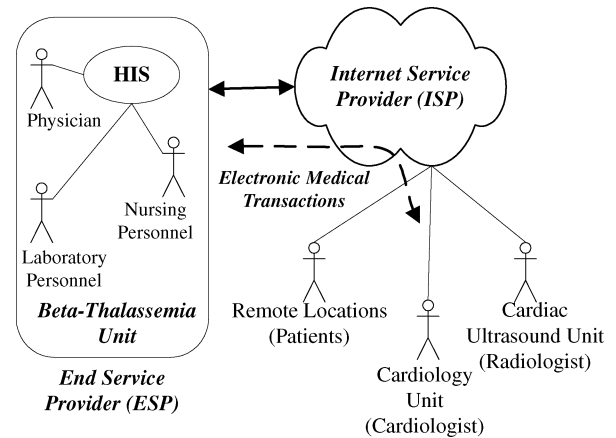

Fig. 1. High-level picture of a shared care environment scenario.

- Electronic communication of examination results between general practitioners and medical laboratories.
- Emergency consultation.
- Home monitoring.
- Insurance claims.

As far as the *actors* (users) of the system are concerned, the following categories have been identified.

A. Clients

In the current context the term "Clients" describes the "patients," since they are the persons utilizing the offered services.

B. Other Stakeholders

Distant or local physicians, hospital employees (nursing and laboratory personnel), insurance agents, and other stakeholders are also considered as users of the system, since they can intimidate the privacy of patients by accessing and/or disseminating parts of their personal medical information.

C. Internet Service Provider (ISP)

The entity providing the infrastructure (hardware and possibly applications) for facilitating access to the Internet services.

D. Telecommunications Provider

The entity providing the physical communication channels i.e., digital or analog lines, signal retransmission equipment using digital centers, satellites, etc. These entities are often big telecommunications organizations.

E. End Service Provider (ESP)

The entity acting as the main healthcare provider. For instance, in the beta-thalassemia scenario, the ESP role is undertaken by the beta-thalassemia unit.

An additional actor, who, although not directly involved in the on-line transactions, plays an important role in carrying out telemedical services, is a Trusted Third Party (TTP) acting as a Certification Service Provider (CSP) [18]. Such entities supply technically and legally reliable means for protecting the data and for producing objective evidence during electronic transactions, using public-key cryptography techniques. TTPs are op-

erationally connected through chains of trust, usually called certificate paths, realizing a web of trust known as Public Key Infrastructure (PKI). The PKI consists of one or several TTPs that generate cryptographic key pairs (private-key, public-key), and issue and revoke certificates for users and other TTPs. These certificates include public-keys, which are used both during verification processes with digital signatures and for the implementation of various encryption mechanisms. In telemedical services, a TTP can be used for generating, distributing, and revoking certificates to patients, medical practitioners, and healthcare organizations that wish to communicate in a secure way.

IV. RISK ANALYSIS AND MANAGEMENT METHODOLOGY

Similarly to any information system, Health Information Systems (HIS) are threatened by both accidental events and deliberate actions. In all cases, the fundamental security attributes of the information, namely *integrity* (prevention of unauthorized modification), *availability* (prevention of unauthorized withholding), and *confidentiality* (prevention of unauthorized disclosure) need to be protected.

Risk analysis (RA) is a sound methodology toward the establishment of a secure information system. RA tackles the security problems and assists the analysts to select the countermeasures that will ensure, in a cost-effective manner, a security level analogous to the level of risks (see Fig. 2). The risk analysis method employed for the shared care scenario under consideration was the CCTA Risk Analysis and Management Methodology (CRAMM) [19]. Its main stages are the following.

1) *Identify and Valuate the Assets of the Information System*: Main assets are the equipment, the applications, and the data. All of them have a value that can be either their purchase price (e.g., a computer system) or the price for reconstructing the asset (e.g., rebuild a custom-made application). The value of an asset depends on the impact that will be caused to its owner if it is damaged.
2) *Identify and Assess Threats and Vulnerabilities*: The threats faced by the information system can exploit certain system vulnerabilities and, thus, cause a security incident.
3) *Risk Assessment*: The combination (threat, vulnerability, impact) for an asset of a specific value provides a measure of the risk level to which this asset is exposed. The derived risk levels are assessed in order to select—in a cost-effective and justifiable way—the appropriate countermeasures.

V. RISK ASSESSMENT

This section summarizes the results of the risk assessment for the beta-thalassemia scenario described earlier. Due to space limitations, no detailed description of the asset valuation and the threat–vulnerability assessment stages are provided. Instead, only the cases exhibiting a high risk level, as a result of a threat with a high probability to occur and a serious system vulnerability, for the patients' medical and personal data are described below. The correspondence between the risk assessment results (high-risk cases), the security incidents that have been reported over a five-year period, and the impact caused are presented in
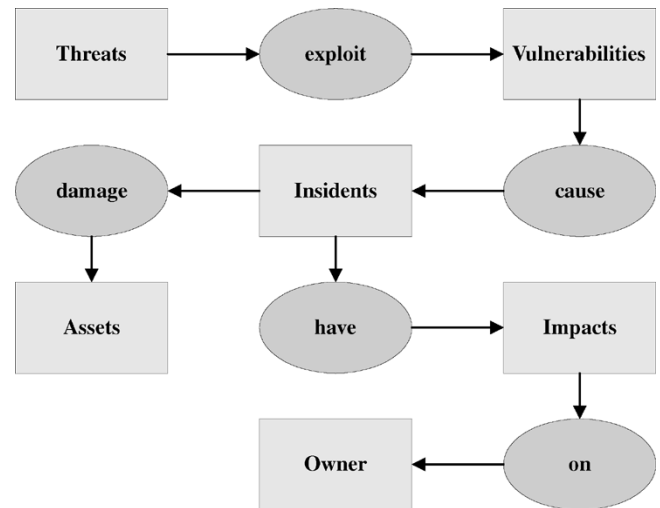

Fig. 2.   Risk analysis methodology.

Table I. This same table provides information about the relative frequency of appearance of each security incident [20], [21].

A. Authorization Problems in Diverse Environments

Patients suffering from chronic diseases, such as beta-thalassemia, are in need of repeated follow-up investigations and continuous treatment, as clearly highlighted in Fig. 1. In such a diverse environment, ensuring that only authorized persons can access the personal data of the patient becomes increasingly difficult and complex.

B. Distant Access Risks

In the aforementioned shared care scenario, several healthcare professionals may be located at distant medical units. In such cases wide area networks, including the Internet, are required for transferring extracts of patient records, which endangers security. Electronic Healthcare Record applications may be standalone, in which case they are responsible for communicating record contents, or web-based, which by default allow remote accessing of central record databases. In both cases, they should implement adequate security measures for protecting patient information.

C. Access to Mobile Information Storage During Emergency Situations

Patients themselves demand that important information on their medical conditions (medical record summaries) are stored on smart cards, which they can carry and present in case they need medical assistance. Although healthcare professionals should normally read smart card contents after being authorized by their owners, in case of emergencies it may not be possible to obtain authorization. Patients then lose control of who accesses their personal information.

D. Central Information Storage Attacks

Medical records are stored in central repositories (HIS), at an institutional level, and can be easily accessed over the Internet by remote healthcare professionals that patients visit only occasionally. Even though such repositories are very useful, they

TABLE I
RISK ASSESSMENT RESULTS

"High Risk" Cases (Security Concerns)	Related Security Incidents		Impact
	Frequency	*Main "Threats" Held Responsible*	
Authorization problems in diverse environments / Distant access risks	15 %	Masquerading User Identity Unauthorised Use of an Application Accidental Mis-routing Introduction of Malicious Software	Patient embarrassment; Loss of trust; Legal consequences; Loss of reputation
Access to mobile information storage during emergency situations	7 %	Failure to comply with personal data protection rules and guidelines	Patient embarrassment; Legal consequences
Central information storage attacks	65 %	Technical Failure of a Host System / Storage Facility / Network Component Misuse of System Resources Introduction of Malicious Software Masquerading User Identity Unauthorised Use of an Application	Patient embarrassment; Poor quality of services; Insufficient patient treatment; Legal claims; Financial impact; Loss of trust; Loss of reputation
Dissemination of research information / Ownership of medical records dilemma	3 %	Failure to comply with personal data protection rules and guidelines	Legal consequences
Communication channels monitoring / tempering	2 %	Communications Infiltration	Insufficient or inappropriate patient treatment; Poor management; Financial loss
Collection of profiling information	3 %	Failure to comply with personal data protection rules and guidelines	Privacy Violation, Legal consequences
Violation of 'Least Information Flow' principle	5 %	Failure to comply with personal data protection rules and guidelines	Legal consequences

put in danger the confidentiality and integrity of medical information, since they offer their services to multi-user, inter-networked environments, which can be easily attacked.

E. Dissemination of Research Information

Maintaining Electronic Healthcare Record repositories is also a prerequisite for optimizing medical services. Improving the management of blood supplies at national level is an example. Conduction of medical research is an additional driving force for the development of centralized patient record databases. In such scenarios, the protection of sensitive personal information is a challenging task.

F. Ownership of Medical Records Dilemma

In several countries, medical records belong to the healthcare units creating them, rather than to the patients they pertain to. In these countries the healthcare professionals that are responsible for maintaining parts of the records often deny sharing information with their colleagues, in an attempt to protect their own research. In such cases, further to safeguarding personal patient data, medical information systems should also protect the intellectual property of healthcare professionals.

G. Communication Channels Monitoring

During electronic medical transactions, the patients always face the man-in-the-middle risk. That means that somebody may act as an eavesdropper and monitor/record all the traffic exchanged through the communication channel. In such cases, the identity of the patient can be revealed and/or the confidentiality of the data may be compromised.

H. Communication Channels Tampering

The information transmitted over a communication channel can be deliberately or accidentally modified, thus sacrificing data integrity.

I. Collection of Profiling Information

ISPs can easily generate a "user profile" by gathering information on how often her/his medical data are accessed and the type of electronic medical transactions she/he normally performs.

J. Violation of "Least Information Flow" Principle

Whenever a patient is requested to provide specific personal and/or medical information, she/he runs into the danger of revealing much more information than it is really necessary for the specific task she/he is trying to complete.

VI. RISK MANAGEMENT

Following the risk identification and assessment for the beta-thalassemia shared care scenario, it is now essential to manage the risk by employing a set of security measures (countermeasures) that enhance the security of communication channels and safeguard the anonymity and secrecy of internet users [11], [22]. Emerging technologies for the former case are known as information security technologies (ISTs) whereas for the latter case are known as privacy enhancing technologies (PETs).

A list of countermeasures (based on ISTs and PETs), suitable for the shared care environment addressed in this paper, has been compiled for each actor category and is presented below. It should be emphasized that the majority of the countermeasures

included in this list are also applicable to many other electronic medical environments, pertaining to chronic and acute diseases, as most of them share many common characteristics with the beta-thalassemia scenario. Capitalizing on this fact, and in order to facilitate the easy adoption of the results to other similar medical environments, the security measures are presented as *general technical guidelines* for modern electronic medical environments, rather than specific countermeasures for the beta-thalassemia scenario.

A. Protection Measures and Practices on the Client's Side

As already stated, the term "Client" describes a patient performing an electronic medical transaction. Considering that countermeasures cannot be implemented under the sole responsibility of patients, it is important to guarantee that the service providers (for instance health care organizations) will support them. Nevertheless, even in such cases, the patients must be aware of the existence and the purpose of such countermeasures, in order to evaluate the overall security level of the provided electronic medical services.

Use of Secure Communication Technology: Employ all appropriate means for protecting the confidentiality and integrity of the personal and medical data transmitted over a communication channel. Such means include strong authentication methods, beyond the basic password-based techniques, such as certificate-based authentication (e.g., X.509 certificate handshaking within SSL) challenge-response methods [e.g., Challenge Handshake Authentication Protocol (CHAP)] or smart card based mechanisms [e.g., Extensible Authentication Protocol (EAP)]. The establishment of cryptographic end-to-end secure sessions that mitigate the risks within the ISP and the telecom providers is also required (e.g., the Secure Sockets Layer (SSL) protocol [23], implemented on the transport layers, providing data confidentiality and integrity protection to the application level protocols, being http, smtp, ldap, etc.).

Moderate Disclosure of Personal Data: The clients should pay particular attention to the disclosure of personal information while navigating through various nontrusted medical applications and/or web sites. Such information may concern.

- Personal identification data such as name, contact details, Social Security codes, or sensitive medical details, collected with the user's consent, through HTML forms, e-mail, or by other means.
- Information collected without the user's knowledge, as imposed by the communication protocols or demanded by the application. Such information may include, but is not limited to, network addresses, information stored in cookies, plug-ins installed on the client machine, and "web page referrers" that may disclose previously visited URLs. Although most of the time the transmission of such information is unavoidable, the flow can be limited to the absolute minimum, by disabling client-side scripting (e.g., Java VM) and by configuring the security settings of web browsers.

Seeking Anonymity: Employ all appropriate mechanisms and procedures for ensuring anonymity to the extent dictated by the applicable law. If anonymous access is not allowed by the application, there are many mechanisms ensuring anonymity, such as the use of pseudonyms or other protocols based on blind digital signatures and public-key cryptography (usually on Diffie–Hellman algorithm) mostly implemented in anonymous electronic cash systems [24]. In the case where full anonymity is not allowed by law, the correlation between a pseudonym and a real person must be disclosed only to trusted entities. A CSP may act as an "anonymity service provider" by issuing digital certificates with pseudonames, while it is committed to disclose the identity of the certified entity upon any official request.

Adhere to the "Least Disclosed Data" Principle: Reveal only data that are necessary for the attainment of the purposes pursued through the particular communication. Unjustified requests for disclosure of information, with emphasis on sensitive data that is not related to the scope of the communication, must be explicitly denied by the client [4].

Cautious Use of E-Mail Distribution Lists: The dispatch of information to mailing lists usually conceals significant risks, such as the receipt of the information by unknown entities or the storage of the messages in public mail archives. The e-mail address itself constitutes personal information and falls under the same protection level as all other personal data. Therefore, one should only participate or use e-mail distribution lists that are clearly functioning as "moderated," i.e., that are used and managed by a closed group of people. Additionally, an unsubscribe process must be provided and the entities participating must be explicitly notified about the purpose of collection, the processing duration and the potential recipients of the information. A recent internet-draft proposes the "Authenticated Mail Transfer Protocol" (AMTP) as a secure alternative of the SMTP. A further evolution on this effort will solve many of the security problems related to the usage of mailing lists.

Control Local Code Execution for Remote Applications: Several medical content providers may adhere to the Application Service Provision (ASP) model or the client/server model. In the latter case, the ESP provides the requested medical information through specific software modules that are downloaded to the client machine, such as Java Applets, ActiveX components, or Scripting languages. Particular attention should be paid while downloading and executing remote software, in respect to its authenticity, its quality, and its content. In other words, the origin of the software must be validated (e.g., by means of digitally signed code, by trusted vendors), the lack of malicious parts or bugs must be assured (e.g., by means of heuristic antiviral methods), and finally the software must be tested against the unnecessary collection and processing of personal data.

Control Cookies: Cookies are files stored in the client's machine while the user is navigating through the world wide web. They are used for storing personalized navigation attributes, user profiling information, http "session variables," and data entered through HTML forms, including passwords in protected form. The information stored is used throughout the duration of a session with a web site or for future visits in the same site for the adaptation of a web server to the specific user preferences. The complete restriction of cookies is usually impossible, since it would prevent opening an authenticated session with

many web applications. However, the frequent manual deletion of cookies stored in the local machine may be used as a countermeasure.

Be Aware of Applicable Legislation: Users should be aware of the latest legislation framework guidelines related to the protection of personal data processing and communication.

B. Protection Measures and Practices on the Internet Service Provider's Side

The ISPs support the electronic medical environment *at the network level*. Since this paper focuses on Clients and End Service Providers, the actions an ISP should consider are only briefly listed below. A more detailed description can be found in [25].

Support Secure Communication: There are several techniques and methods that can be combined by an ISP for ensuring secure communication. As a recommended practice, the ISP should deploy a Remote Authentication Dial-In User Service (RADIUS) supporting EAP and LDAP authentication as well as additional measures for securing the critical communication services, being the TCP/IP, the Domain Name Service (DNS), and the routing protocol such as the BGP.

Support Secure Content Hosting: A frequently used model for the provision of large volumes of content, such as medical data, is its hosting at an ISP's data center. For efficiency purposes, the data may be distributed in different locations, thus preventing network bottlenecks.

Protect Cached Data: Another case of medical data archiving at an ISP side is that of caching. The data stored in proxies and cache boxes must be protected in a way similar to that described in the previous paragraph.

Provide the Tools for Secure Communications: The ISPs should inform and, if possible, facilitate the users to acquire the necessary tools for establishing secure communications either at the Network layer (e.g., L2TP Layer 2 Tunneling Protocol), or at the Internet layer (e.g., IPSEC), or above the Transport layer (e.g., SSL Secure Sockets Layer), or at the Application layer (e.g., S-HTTP, SSH Secure Shell), or above the Application layer (e.g., PGP keys management software, S/MIME clients).

Perform a detailed risk analysis study in order to identify all possible threats to the Information System, decide and implement the appropriate security measures, and develop a specific security policy.

Develop an ethics code on the protection of personal data that will be based on the provisions of the 95/46, 97/66, and 2002/58 Directives and which shall be notified to the management and all staff.

Unconditional Access to Personal Data: The ISP should facilitate the unconditional access of clients to their own personal data, through dynamically produced web content by means of server-side scripting technologies. The necessary access-control mechanisms should be based on the Mandatory Access Control (MAC) model that achieves the strongest security level for individuals.

Policy Publication: Publicize, by all available means, the privacy policies adopted pursuant to 95/46 Directive and the applicable national law.

Transparent Data Collection: The process of gathering client information must be transparent. Specifically, the data collected should be limited to those that are absolutely necessary for the conclusion of the contract between the subscriber and the ISP.

Contract Information Protection: The ISP should employ all appropriate security measures for protecting the personal data gathered for the conclusion of the contract between the ISP and the client, including pseudonyms, passwords, and billing information. Such information must be protected during its transmission through communication channels (e.g., by means of certificate-based authentication and data encryption) and at its physical and logical storage area (e.g., by means of Mandatory Access Control (MAC) policies).

Protection Level Compatibility: ISPs should avoid transferring personal and/or sensitive information (including medical data) to non-EU countries or to third countries that do not guarantee a protection level compatible to that of European member states.

Promote Anonymity: Encourage and provide appropriate technological means for achieving anonymous communications [26], [27].

Aggregate Information Logging: Avoid monitoring and/or recording user communications, unless this is necessary for billing purposes. Even in the latter case, the logged data must be limited to aggregated or statistical information.

User's Consent: In cases where recording is a prerequisite for the provision of specific user services (e.g., proxy services), the inherent risks must be communicated to the users. The use of such services must be allowed only after obtaining the user's explicit consent.

Third Party Links and Applications: Control the web applications hosted (such as banners) in respect to the personal information that they can intercept in case the user selects and uses one of them. As a common example, the "URL referrer" is usually collected by the banner owner, while it may contain personal information posted in a previously visited web page.

C. Protection Measures and Practices on the Telecommunication Providers' Side

A telecommunication provider maintains and offers the communication media (channels) for the interconnection of all interested parties. The identification of protection measures for such providers is outside the scope of the paper, since none of the actors involved in a medical environment (i.e., clients, ISPs, ESPs, etc.) can enforce specific security mechanisms. These are under the sole responsibility of the telecom provider. However, since the security level realized can seriously affect the protection of sensitive medical information transmitted over the communication channels of the provider, it is worth mentioning some generic guidelines that they should follow.

- Perform a detailed risk analysis study in order to identify all potential threats to the Information and Communication Systems they use.
- Decide on and implement the appropriate security measures.
- Develop and maintain a specific security policy.

Following the above guidelines ensures that the physical and logical security of the communication services offered by the Telecommunications Providers will be in accordance to the 95/46 and 2002/58 Directives.

D. Protection Measures and Practices on the End Service Provider's Side

At the *application level* of an electronic medical environment, the ESPs support the required functionality for electronic medical transactions. The majority of the protection measures proposed for an ISP, regarding the protection of sensitive hosted or cached data, the publication of policies and practices, the anonymity, and the collection of personal information, are also applicable for an ESP. Some additional requirements are listed next.

Preliminary Agreement: During the registration stage, the ESPs should clearly inform the user about the services they offer together with the conditions for their use, obtaining at the same time the user's consent. Specifically, for on-line "user agreements" the following should apply.

- The agreement should be clear, comprehensive, and free of any ambiguous terms.
- Only the transactions explicitly listed in the agreement should be realized.
- The user should have an unconditional option to withdraw.

Control End-to-End Security: Security requirements should not be limited to data repositories and communication channels. Considering modern medical applications, based on the N-tier model, there is a clear need for employing security mechanisms for all stages of data storage, data transformation, and data transmission. Therefore, the protection measures should be applied to databases, transaction servers, application servers, web servers, and to any other intermediate tier, including their inter-communication, even if they are located at the same physical site.

Patient Records Access Standards: Several standardization bodies, including CEN and HL7, have proposed Electronic Healthcare Record architectures that address the issues of user authorization, access permissions to the various sections of the record, and exchange of medical data between different applications [28], [29]. Thus, Electronic Healthcare Record applications that comply to such standards can much more easily accommodate the additional security mechanisms required for the support of a medical service. The necessary access-control mechanisms should be based on the Role-Based Access Control (RBAC) model that combines the highest security level with efficiency, for group access control (e.g., groups of physicians, healthcare personnel, and insurance companies).

Employ Moderated Mailing Lists: Mail distribution lists are often a valuable mean for disseminating information between ESPs and clients. Every mailing list that includes client addresses and is owned by an ESP must be moderated, having strictly controlled usage permissions and providing to the end users the option to withdraw.

Do not downgrade the functionality offered to a user as a result of her/his denial to fill in noncompulsory fields of the registration form or due to restrictions on her/his machine, such as blocking cookies, content filtering, and denial of script execution.

E. Protection Measures and Practices for Other Stakeholders

Considering the remaining stakeholders (i.e., distant or local physicians, nursing and laboratory personnel, insurance agents, etc.), strong authentication and authorization mechanisms are necessary for protecting patients' privacy. Specifically:

Strong Authentication Mechanisms: Employ strong authentication technologies, such as EAP or PKI-enabled smart cards, possibly in conjunction with biometric techniques, in order to validate the credentials of the involved stakeholders, either locally or remotely.

Strict Access Control Policies: The Role-Based Access Control (RBAC) model is suitable for medical environments, since it establishes the access privileges of a user according to its role (e.g., physician, nurse or researcher). The Mandatory Access Control (MAC) model may also be utilized for ensuring that any individual other than the owner cannot downgrade private information to a lower confidentiality level.

Hidden Identity of Data Owners: Unless absolutely necessary, the identity of the users owning specific medical information should not be disclosed. Aggregate information or anonymous data are in most cases sufficient for research and other purposes.

Least Information Disclosure: The information disclosed to a third party must be kept to the absolute minimum, depending on the role of the stakeholder. For example, a nurse should grant access only to the information required for a specific treatment and not to the entire medical history of the patient.

F. Protection Measures and Practices for Trusted Third Parties

A TTP and its services are only indirectly involved in an on-line transaction by having pre-established the necessary trust relationships between the involved parties. They contribute to the effort of preserving the constituent elements of an electronic medical environment (namely data, equipment, software, procedures, etc.) as well as controlling the access of the stakeholders. A TTP is by definition "Trusted" for its operations and this is the key of its existence. In general terms, a TTP is trusted by its clients for the accuracy of the binding between a digital certificate and a physical entity. It is also trusted for the accuracy, the integrity, and the availability of any data provided to support secure communications, such as time-stamps, Certificate Revocation Lists, and Directories. Furthermore, a quality-certified TTP [30] will inspire the global trustworthiness needed in a medical environment and, thus, will provide the means to apply global and strict security policies. The security services offered by a TTP mainly aim to fulfill the security requirements imposed by the electronic services offered to users, namely authentication, data integrity, confidentiality, nonrepudiation, anonymity, key management, time-stamping, and publication of the Certification Practice Statement.

Specifically for the case of electronic medical environments, a TTP should fulfill/comply with the following.

Formation of Global Trust Architectures: The TTPs involved should be part of widely accepted trust architectures, such as global hierarchies, bridged Certification Authorities (CAs), or

TABLE II
RISKS AND COUNTERMEASURES CORRESPONDENCE

Risks for Patients in an Electronic Medical Environment (in terms of Privacy Violation) / Proposed Countermeasures	Authorization problems in diverse environments	Distant access risks	Access to mobile information storage during emergency situations	Central information storage attacks	Dissemination of research information	Ownership of medical records dilemma	Communication channels monitoring	Communication channels tampering	Collection of profiling information	Violation of 'Least Information Flow' principle
Clients										
Use of secure communication technology		X		X			X	X		
Moderate disclosure of personal data			X	X	X	X			X	X
Seeking anonymity				X	X	X	X		X	
Adhere to the 'Least Disclosed Data' principle			X	X	X					X
Cautious use of e-mail distribution lists				X			X			
Control local code execution for remote applications	X	X		X						X
Control cookies		X		X			X		X	X
Be aware of applicable legislation	X	X	X	X	X	X	X	X	X	X
ISPs										
Support secure communication		X		X	X		X	X		
Support secure content hosting				X						
Protect cashed data				X						
Provide the tools for secure communications		X		X			X	X		
Perform risk analysis	X	X		X	X	X	X	X	X	X
Develop an ethics code	X	X		X	X	X	X	X	X	X
Unconditional access to personal data	X					X				
Policy publication		X		X		X			X	X
Transparent data collection				X					X	
Contract information protection				X					X	
Protection level compatibility	X	X		X			X			
Promote anonymity				X	X	X	X		X	
Aggregate information logging				X	X	X			X	X
User's consent	X		X	X	X					
Third party links and applications				X			X	X	X	
ESPs										
Preliminary agreement			X	X		X			X	
Control end-to-end security	X	X		X			X	X		
Patient records access standards		X	X	X		X				X
Employ moderated mailing lists				X			X			
No functionality downgrade		X							X	X
Other stakeholders										
Strong authentication mechanisms	X	X		X						
Strict access control policies	X			X		X				
Hidden identity of data owners			X	X	X	X				
Least information disclosure			X	X	X	X			X	X
TTPs										
Formation of global trust architectures	X	X	X	X						
Key management				X			X	X		
Anonymity				X						
Smart cards employment	X	X	X	X						

cross-certified CAs. Consequently, the digital certificates issued by the TTP will be trusted by the entire medical community, enabling also strong off-line authentication procedures, which are critical for urgent off-line access to locally stored medical data.

Key Management: The TTP should employ the appropriate software and/or hardware for providing users with the option to utilize private key(s) for data encryption and digital signatures. Currently, the available options are as follows.

- Creation of the private key by the software installed at the user's machine [22] with the TTP simply certifying her/his public key. Normally this is the procedure followed for the creation of keys utilized for personal IDs and digital signatures, since the private keys must remain under the absolute control of their owners.
- Creation of the user's private key from the software installed at the TTP's computing system. In this case, the TTP operates as a Key Management Center (KMC) and delivers the certificate and the private key to the subscriber via a transferable storage medium [22]. The storage of the private key at the TTP side, for recovery reasons, should constitute an additional service offered by the TTP. Such service, though, should be in the discretion of the subscriber.

Anonymity: The TTP must be in a position to issue anonymous certificates for carrying out anonymous transactions. In such cases, TTPs are responsible for ensuring the secrecy of the one-way correlation between the subscriber and the nickname she/he uses. The techniques employed by the TTP for fulfilling the above requirement should be included in the privacy protection policy.

Smart Cards Employment: Smart cards constitute a highly secure, tamper-proof and mobile device for storing the private keys of the clients and other stakeholders. As a result the TTP should be able to support the use of smart cards for authentication and authorization purposes, either remotely or locally and even in off-line applications.

The aforementioned protection measures and practices can efficiently eliminate the privacy violation risks presented in Section V. The correspondence between potential risks and countermeasures is summarized in Table II. The same table highlights the fact that specific countermeasures can be utilized autonomously or they can be combined with other countermeasures.

VII. CONCLUSION

In modern "digital societies," privacy and confidentiality remain important values to the human psyche. The protection of personal information and/or sensitive medical data, within the framework of electronic medical transactions, constitutes a crucial factor for the successful attainment of Information Society's purposes. In order to protect the personality of an individual from being offended, all entities-actors (Users/Patients, ISPs, Telecommunications Providers, ESPs, and TTPs) involved in an electronic transaction should employ the appropriate organizational, procedural, and technical countermeasures. As far as the technical countermeasures are concerned, they mainly focus on ensuring the security of the communication channels, protecting the anonymity of the users, protecting the confidentiality of the information through encryption, supporting digital signatures, etc. On the other hand, the organizational and procedural countermeasures are equally important since they are closely linked to the legal and regulatory framework governing the issues of "privacy protection" and "protection of personal and, especially, sensitive data." Within the evolving telemedicine framework, it is a clear necessity that all involved entities must be constantly informed on the aforementioned issues, thus enabling them to adopt the appropriate set of countermeasures. This is the only way that telemedicine services can be further developed, while respecting "patients" in the digital era.

REFERENCES

[1] *The ISHTAR Consortium, Implementing Secure Healthcare Telematics Applications in Europe*, IOS Press, Amsterdam, The Netherlands, 2002.
[2] (1998) A little Net privacy please. Business Week. [Online]. Available: http://www.businessweek.com
[3] "On the convention for the protection of individuals with regard to automatic processing of personal data," The Council of Europe, Convention no. 108, 1981.
[4] "On the protection of individuals with regard to the processing of personal data and on the free movement of such data," The European Parliament and the Council of the European Union, Directive 95/46, 1995.
[5] "On the protection of individuals with regard to the processing of personal data in the telecommunication sector," The European Parliament and the Council of the European Union, Directive 97/66, 1997.
[6] "On the protection of medical data," The European Parliament and the Council of the European Union, Recommendation R(97)5, 1997.
[7] "Privacy and electronic communications: Processing of personal data and the protection of privacy in the electronic communications sector," The European Parliament and the Council of the European Union, Directive 2002/58, 2002.
[8] B. Blobel and F. Roger-France, "A systematic approach for analysis and design of secure health information systems," *Int. J. Med. Inform.*, vol. 62, no. 1, pp. 51–78, 2001.
[9] S. Gritzalis, J. Iliadis, D. Gritzalis, D. Spinellis, and S. Katsikas, "Developing secure web-based medical applications," *Med. Inform. Internet Med.*, vol. 24, no. 1, pp. 75–90, 1999.
[10] S. Fischer-Hubner, *IT Security and Privacy*. Berlin, Germany: Springer-Verlag, 2001, vol. 1958, Lecture Notes in Computer Science.
[11] A. Ghosh, *Security and Privacy for E-Business*. New York: Wiley, 2001.
[12] J. Argyrakis, S. Gritzalis, and C. Kioulafas, "Privacy enhancing technologies: A review," in *Proc. EGOV03 2nd Int. Conf. Electronic Government*, vol. 2739, Lecture Notes in Computer Science, R. Traunmuller, Ed., Prague, Czech Republic, 2003, pp. 282–287.
[13] (1999) Privacy and human rights—An international survey of privacy laws and developments. Privacy International, Electronic Privacy Information Center. [Online]. Available: http://www.privacy.org/pi/survey
[14] S. Warren and L. Brandeis, "The rights to privacy," *Harvard Law Rev.*, vol. 5, pp. 193–220, 1890.
[15] R. Rosenberg, *The Social Impact of Computers*. New York: Academic, 1992.
[16] "Implementing the OECD privacy guidelines in the electronic environment: Focus on the Internet," OECD, DSTI/ICCP/REG(97)6/FINAL, 1998.
[17] S. Deftereos, C. Lambrinoudakis, and D. Gritzalis, "High level security policies for health: From theory to practice," in *Proc. Electronic Health Record Security Workshop, Int. Congr. Medical and Care Compunetics (ICMCC)*, The Hague, The Netherlands, 2004, pp. 416–423.
[18] S. Gritzalis, D. Gritzalis, K. Moulinos, and J. Iliadis, "An integrated architecture for deploying a virtual private medical network over the web," *Med. Inform. Internet Med.*, vol. 26, no. 1, pp. 49–72, 2001.
[19] *CCTA Risk Analysis and Management Methodology*, U.K.: Central Computer and Telecommunication Agency, 1997.
[20] S. Deftereos *et al.*, "Developing a security plan for a distributed beta-thalassemia information system," (in Greek), Laiko Hospital, Tech. Rep., 2002.

[21] S. Deftereos, C. Lambrinoudakis, P. Andriopoulos, D. Farmakis, and A. Aessopos, "A Java-based electronic healthcare record software for beta-thalassaemia," *J. Med. Internet Res.*, vol. 3, no. 4, 2001.

[22] C. Lambrinoudakis and S. Gritzalis, "Managing medical and insurance information through a smart card based information system," *J. Med. Syst.*, vol. 24, no. 4, pp. 213–234, 2000.

[23] A. Freier, P. Karlton, and P. Kocher, *SSL ver. 3.0*: Netscape Communications Corp., 1996.

[24] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in *Proc. Crypto'88—Advances in Cryptology*, vol. 403, Lecture Notes in Computer Science, Santa Barbara, CA, Aug. 1988, pp. 319–327.

[25] S. Gritzalis, "Enhancing privacy and data protection in electronic medical transactions," *J. Med. Syst.*, vol. 28, no. 6, pp. 535–547, Dec. 2004.

[26] A. Froomkin. (1996) Flood control on the information ocean: Living with anonymity, digital cash and distributed databases. Univ. Pittsburgh Journal of Law and Commerce. [Online]. Available: http://www.law.miami.edu/~froomkin/articles/oceanno.htm

[27] S. Gritzalis, "Enhancing web privacy and anonymity in the digital era," *Inform. Manage. Comput. Security*, vol. 12, no. 3, pp. 255–287, Mar. 2004.

[28] "Health informatics: Electronic healthcare record architecture," CEN TC251/WG1, ENV 13606:1999.

[29] (2000) Patient record architecture. KONA Editorial Group. HL7 Document. [Online]. Available: http://www.hl7.org/special/committees/sgml/PRA/PRA_ballot_April00.zip

[30] D. Lekkas, S. Gritzalis, and S. Katsikas, "Quality assured trusted third parties for deploying secure internet-based healthcare applications," *Int. J. Med. Inform.*, vol. 65, no. 2, pp. 79–96, May 2002.

Costas Lambrinoudakis was born in Greece in 1963. He received the B.Sc. degree in electrical and electronic engineering from the University of Salford, Salford, U.K., and the M.Sc. degree in control systems and the Ph.D. degree in computer science from the University of London, London, U.K.

Currently, he is an Assistant Professor in the Department of Information and Communication Systems, University of the Aegean, Samos, Greece. His current research interests include information systems security, smart cards, and computer architectures. He is an author of several refereed papers in international scientific journals and conference proceedings.

Dimitrios Lekkas was born in Greece in 1969. He received the B.Sc degree in mathematics from the University of Athens, Athens, Greece, the M.Sc. degree in information technology from Glasgow University, Glasgow, U.K., and the Ph.D. degree in information systems security from the University of the Aegean, Syros, Greece.

Currently, he is a Lecturer in the Department of Product and Systems Design Engineering, University of the Aegean, Syros, Greece. His current research interests include computer security, incident response, public key cryptography, database management systems, and distributed systems. He has published several refereed papers in international scientific journals and conference proceedings.

Stefanos Gritzalis was born in Greece in 1961. He received the B.Sc. degree in physics, the M.Sc. degree in electronic automation, and the Ph.D. degree in informatics from the University of Athens, Athens, Greece.

Currently, he is an Associate Professor in the Department of Information and Communication Systems Engineering, University of the Aegean, Samos, Greece, and Assistant Director of the Info-Sec-Lab. His published scientific work includes six books (in Greek) on information and communication technologies topics, and more than 70 journal and national and international conference papers. The focus of these publications is on information and communication systems security.

Spyros Deftereos was born in Greece in 1973. He received the MD and Ph.D. degrees in medical informatics from the University of Athens, Athens, Greece. His work focused on improved healthcare services using diagnosis support systems.

He worked at the School of Medicine, University of Athens, and participated in European projects related to telematics in healthcare, patient record management, and related subjects. He has published extensively in the international literature on areas such as thalassemia and applications of computer analysis of patient records.