Gattiker, U. E., Fahs, R., Blaha, J. & members of EICAR Working Group 1. (2000). Managing medical information systems: Can patients' privacy be protected or should we simply give up? **International Journal Healthcare Technology and Management**, **2**(1), 1-40.

This paper represents a collaborative effort between the authors and EICAR Ad-Hoc Working Group **Trust in E-Commerce** at:

http://www.EICAR.DK/Trust

This paper is an earlier version of the citation given above. For the published version the reader is asked to look at the publication listed above.

Managing Medical Information Systems: Can Patients' Privacy be Protected or Should we Simply Give up? [1][2]

Urs E. Gattiker
Aalborg University, DENMARK

Rainer Fahs
Jaroslav Blaha
NATO Air Command & Control Systems Management Agency (NACMA), Belgium

in collaboration with members of EICAR[3] Ad-hoc Working Group – Trust in E-Commerce[4]

[1] Please send comments and requests for reprints to Urs E. Gattiker, Obel Family Foundation Professor of Technology and Innovation Management, Department of Production, Fibigerstraede 16, DK-9220 Aalborg, DENMARK. Telephone:+45 981160 40 (mornings only) or +45 222 111 40; Fax: +45 9815-3030; Home Office: +45 222 111 40 (mornings and evenings); E-Mail: WebUrs@WebUrb.dk or for additional information or downloading of this paper please point your browser to: http://Research.WebUrb.dk/ or http://Research.WebUrb.dk/NetProfits

[2] The contents of this article do not in any way reflect opinions of either employer of the three authors. Usual disclaimers apply.

[3] European Institute for Anti-Virus Research (eicar), http://www.eicar.org

[4] This paper is based in part on the online discussions held using Working Group 1's list server during Winter 97/98 through Spring 99. As such it reflects a joint effort between the moderator (first author), Rainer Fahs, Jaroslav Blaha and other group members who contributed in various formal and less formal ways to the content and shape of this report. For EICAR ad-hoc working group Trust in E-Commerce materials pertaining to this topic and related ones, as well as joining EICAR, please check the group's Web site http://www.eicar.dk An earlier version of this paper was presented at the EICAR annual conference in Munich 1998.

Urs E. Gattiker holds the Obel Family Foundation Chair for Innovation and Technology Management (Entrepreneurship) in the Faculty of Engineering and Science at Aalborg University, Denmark. His research interests are in e-commerce, security/safety, anti-virus software development as well as entrepreneurship, gender issues and cross-cultural issues. He has published extensively in these areas.

Rainer Fahs is currently employed as a Senior Information Systems Security Engineer at the NATO Air Command and Control Management Agency (NACMA), where he is responsible for the planning and implementing of IT security mechanism in the project ACCS and the agency. He is also the Chairman of the Board of the European Institute for Computer Anti Virus Research (EICAR).

Jaroslav Blaha is Senior Information Systems Engineer at the NATO ACCS Management Agency. He was chief instructor at the German Air Force Technical Academy, project manager for communications and information systems at the NATO Headquarters AFCENT and Senior Analyst for mission-critical systems at the NATO Programming Centre. He holds university degrees in computer science and economics. Special interests are software engineering aspects of security, standardisation and human-machine interaction

Abstract

Rapid cost escalation in health care have forced governments and associated businesses to reduce or at least contain rising health care costs. One viable approach has been to improve medical record keeping and its accessibility by parties involved in care taking and administration. Divergent stakeholder demands for information and its privacy may result in conflicts between parties (e.g., insurers versus patients). Encryption technology may help to protect the privacy and confidentiality of patients' information. Unfortunately, governments demand to be given the possibility of intercepting and monitoring such electronic data transfer for administrative, legal and law enforcement purposes, should the need arise, is threatening the privacy of patients. This paper reviews these issues and highlights some of the problems and pitfalls various stakeholders are faced with considering medical information, privacy, encryption and law enforcement needs in an international context. Implications for managers and system specialists are described, and how these issues may affect direct marketing, customer databases and electronic commerce is discussed.

Keywords

health care, cryptography, privacy, encryption, costs-benefit analysis, regulation, health cards, digital signature, secret key cryptography

INTRODUCTION

Fiscal restraints and cost cutting by insurers and governments alike has not stopped the rise in health-care costs in North America and Europe. Some suggest that demand for these services will not moderate unless consumers face charges. In turn, these may reduce the escalation of health care-costs, but such charges are unpopular with the public („Coughing up," 1997). A viable option is a better use of technology which can help in improving the management of delivered care and thus reduce the rapidly rising health care costs. To achieve this goal, information systems storing and processing medical records have become of paramount importance. The latter provide a lot of information about an individual's medical history for doctors and medical specialists. In turn, more appropriate health care can be provided thanks to extensive information available to care givers, while duplication efforts for obtaining data and medical history (e.g., when changing one's general practitioner) are reduced. Moreover, the likelihood for giving inappropriate care due to inaccurate information is lowered as well. Finally, prescribing drugs to which a patient might not respond well, or experience undesirable side effects (e.g., nausea), can be reduced by providing the attending physician with a full medical history. In turn, the rapidly escalating costs for prescription drugs could also be managed better.

While medical information may be important to care givers, medical records are also of prime interest to insurers, pharmacists, pharmaceutical firms and medical appliance manufacturers/distributors. These firms can tailor their service and/or marketing efforts better with the help of additional information, while hopefully also reducing their costs. In turn, savings or at least cost containments could be passed on to clients. Naturally, we leave a trail of data behind every time we visit the local health professional. Unfortunately, mischievous intent can always result in such information ending up in the wrong hands. Accordingly, while medical information systems may help in containing the rise in health care costs to some degree, threats to patients' privacy must be carefully considered.

Unfortunately, there has been insufficient research and discussion on issues concerning the development of standards and procedures to protect the privacy of government and business data as well as privacy of consumer information (e.g., data about a person's shopping habits at the local supermarket). While many governments do have standards and procedures for protection of information, they may not necessarily protect an individual's privacy. Moreover, without commonly defining what privacy means for national and international government organizations [e.g., United Nations (UN) and World Trade Organization (WTO)], disagreements and misunderstandings will continue.

When privacy and security matters are addressed in various reports, law enforcement, national security, corporate or consumer issues are usually highlighted (e.g., Szlovits, Doyle, Long, Kohane & Pauker, 1994; The Walsh Report, 1997). All these groups of stakeholders (e.g., expectant and definite stakeholders, such as clients and consumers) have particular interests in mind when discussing privacy and encryption issues. By addressing any group's needs and claims satisfactorily, another stakeholder's rights are likely to be infringed upon. Thus, a careful balance must be found for all primary and legitimate stakeholders to make medical information records a viable option in our attempts to improve health care systems, while protecting the privacy and security of such data.

Appendix 1 outlines some of the terminology used throughout the paper. The purpose of this paper is to:

(1) Discuss both technical and social issues, as far as encryption and privacy of medical records are concerned;

(2) address how various stakeholders' interests can be made more compatible (e.g., governments' requirement for interception and monitoring of electronic data transfer versus patients' demand for privacy);

(3) discuss how these issues may limit our possibilities for reducing health care costs; and,

(4) deliberate some of the practical and research implications including cost benefit issues for protecting medical data.

1. PRIVACY AND ENCRYPTION OF MEDICAL DATA

In this section we discuss the privacy and encryption options available in order to set the stage for the latter part of the paper. Accordingly, the material simply represents an introduction to privacy and encryption (see also Appendix 1 for definition of terms) which is needed to address these concerns as far as medical records are concerned.

1.1. What is Privacy?

Article 12 of the Universal Declaration of the Human Rights (Privacy International, 1996) states that privacy includes one's right to be left alone. The California Supreme Court further reaffirmed this in a decision in Long Beach City (Doss & Loui, 1995). The right to be left alone provides the individual with explicit self-determination about the selection of interpersonal contacts and, most importantly, contacts between organizations and the individual.

The one international agreement governing privacy issues and principles is a document by the Organisation for Economic Co-operation and Development (OECD, November 1980). These guidelines establish principles for the protection of privacy and trans-border flows of personal data for OECD member countries. Specifically, they govern:

- the collection, use, and disclosure of information relating to individuals by **public and private organizations**; and

- access by each individual to information relating to that individual as held/stored by **public and private organizations**.

Most important are the eight principles of privacy as outlined by the OECD, which are:

– collection limitation
– security safeguards
– data quality
– openness
– purpose specification
– individual participation
– use limitation
– accountability

Privacy is also defined as the right to control personal information (Katsh, 1994). This right can be described as control over data, such as credit information (Culnan, 1993). Linking these two approaches, privacy is defined in Appendix 1 of this paper. Accordingly, if the individual does have the right to control personal information, does this, in turn, mean that the owner of the information is able to select protection measures or is it left to the discretion of the agency or firm (e.g., health insurance carrier) to decide? Strong encryption mechanisms and protection measures for the control of transient emanations (TEMPEST) are government controlled in many countries (e.g., USA export control, Wassenaar agreement on export controls for conventional arms and dual-use goods and technologies) (The Wassenaar, December 20 1995). This means that it is technically and economically unfeasible for the individual and for commercial organizations to control and protect their own private data to an extent that they determine themselves and, as importantly, with measures selected at their own discretion. In turn, part of the individual's right to privacy is violated (see Appendix 1 for a definition of the term).

The above indicates that some regulatory and legislative efforts have been undertaken. Unfortunately, privacy protection may be hampered by governments using wrongly defined requirements for national security in order to retain capabilities for their intelligence or law enforcement agencies. This could result in actions that may well go beyond legislative parameters and checkpoints. For instance, Swiss media reported that Swiss police had secretly tracked the whereabouts of mobile phone users via the government-owned telephone company. The latter's computer records provided police with information, going back more than half a year, about subscribers' calls, from where and when calls were made, to how long and to whom these calls were made (Swiss police have, December 28 1997). Worse is that in many people's minds, their legitimate right to access and control their personal information has already been lost. New technologies and large databases facilitate the increasingly effective exploitation of information about consumers and citizens (Schlossberg, 1993).

A massive telecommunications interception network operates within Europe and, according to a new study circulating on the Internet, "targets the telephone, fax and e-mail messages of private citizens, politicians, trade unionists and companies alike." The report says that the network has the ability to tap into almost all international telecommunications as well as parts of domestic phone traffic - and is apparently operated by intelligence agencies without any mechanism of democratic control. The network, dubbed ECHELON, is described in a new study by the European Parliament titled "An appraisal or technologies of political control." The report was written by Steve Wright, an analyst with the Omega Foundation, a British human rights organization, performing work on behalf of the European Parliament section known as STOA (Scientific and Technology Options Assessment) (Giussani, 1998).

The above suggests that total protection of privacy is impossible, and even taking a violator to court can be difficult and expensive (van Swaay, 1995). Moreover, privacy protection requirements are conflicting with those of governmental organizations, such as law-enforcement agencies and intelligence services wishing to retain the capability to access any information at any time, with no notice to its owner. In addition, invasion of privacy is often also the result of conflicting interests in the commercial world. Direct marketing firms try to exploit personal information about consumers, but the consumer is generally not consulted for agreement and in most cases would prefer to be left alone. To illustrate, if a client calls a restaurant to order dinner for home delivery, the restaurant may obtain the telephone number through Caller Number Identification (CNID). This telephone number may be stored on a database for marketing purposes (for example, to mail flyers with special offers to the client), or the number may be sold to other organizations such as direct

marketing firms. Blockbuster Videos was taken to court in 1986 for selling data about clients' movie rental preferences (Bloom, Milne & Adler, 1994). Another example is USA News & World Report, which was taken to court for selling subscriber information to interested firms (Avrahami, 1996). Often, firms use negative option selling plans, whereby unless a client refuses the service (e.g., selling of address to marketers or providing ad-on services free for a trial period, thereafter charging the customer a fee), it is assumed one wishes to receive it (i.e., silent acceptance). Firms find the use of such techniques beneficial if it is assumed that the majority of customers are unlikely to reject the offer (Spriggs & Nevin, 1996), although negative publicity and/or customer complaints may result in a firm changing its plans (e.g., The people vs. AOL, Winter 1998). As far as privacy is concerned, some have suggested that it must be implied that the person has chosen to opt out (i.e., not to participate; protect one's privacy), unless one informs the organization otherwise when being asked (see also Section 3.2.2.).

People also differ in how they might feel about certain privacy invasions. For instance, Gattiker, Kelb, Janz, Hosten, Greshake, Schwenteck and Miller (1997) reported that individuals were more concerned about their loss of privacy due to e-mail than to phone calls trying to sell them a product and/or service. Also, people are probably more concerned about unwanted disclosure of their medical and financial data to others, than their preferences about sports or TV-watching habits (see also Appendix 1 for a comprehensive definition for privacy).

1.1.1. Privacy Protection

Selecting the appropriate protection measures will be a challenge for legislators and organizations/private citizens alike. In most countries, with the exception of Pretty Good Privacy (PGP), strong encryption technology and TEMPEST equipment for private or commercial use (see also Sections below such as 3.3.) is either not available, requires a license or is conditioned on key recovery or escrow schemes (see also Appendix 1 for explanation of these terms). Probably worse is that by having access to these technologies, agencies are able to bypass existing laws and regulations without the individual or firm being even aware of it having happened. For instance, the privacy protection act in Germany prohibits the random monitoring and wiretapping of individuals. Unfortunately, if the party does not know that data transfer has been intercepted, and there is absolutely no trace of interception of transient emanations for example, the individual cannot use the law to act against such privacy violations.

1.2. Security of Information Systems and Cryptography

The above sections indicate that privacy issues have come to the attention of the media and the public; however, potential conflicts between private citizens', commercial users' and government agencies' interpretation and protection or violation of privacy are numerous. One of the challenges remaining is how to protect privacy while upholding the public's right to and/or freedom of information (e.g., access to data of interest to the public). The increase of information systems and globalization of business further necessitates efforts to protect data not only for confidentiality, but also for integrity and availability. However, systems and data also become increasingly vulnerable to a greater variety of threats, such as unauthorized and unknown access and illegitimate use, alteration, and/or destruction. Proliferation of computers, increased computing power, interconnectivity, decentralization, growth of networks and the number of users, all increase a system's vulnerability. Some have suggested that systems containing more than 1,000,000 people's records should not be built because confidentiality, integrity and availability requirements cannot be met satisfactorily (Anderson, 1996) (cf. Table 1). Moreover, convergence of information and

communications technologies and our increased dependence on their daily use makes us more dependent upon such systems. For instance, power outage may result in a pharmacy being unable to process transactions because its information systems are no longer functioning. A care team may not be able to access a patient's record if the data transfer from a centralized system is interrupted. This could, unfortunately, reduce the quality of care provided by the medical team.

Security of information and communications systems involves the protection of the **confidentiality, integrity and availability** of those systems and the data that is processed, stored or transmitted on them. Table 1 lists these properties and provides explanations. While in theory the three properties are manageable, natural disasters such as the large power outage for areas of Québec in 1997/1998 (some areas where without power for more than three weeks) show that upholding the properties is often difficult. For instance, diesel generators may work fine for a few hours, but fail to perform at high output for several days. As the Québec experience shows, this might result in data no longer being available or some rural hospitals having to shut down for a period.

Insert Table 1 about here

The relative priority and significance of confidentiality, integrity and availability vary according to the information or communication systems and the ways in which those systems are used. The quality of security for storage and transmission of data with information systems depends not only on hardware, software and other technical measures used, but also on good managerial, organizational and operational procedures (see Gattiker and EICAR WG 1, 1997 for an extensive discussion of these issues).

The growth and commercial development of public networks, such as the Internet, depends on solving the question of trust. As Table 1 suggests, confidentiality of data may be enhanced with cryptography. Data transfer increases risks against data integrity unless cryptography prevents unauthorized parties to alter data when being transmitted from A to B. Hence, cryptography is an important component, helping to make an information and communications system more secure, and ensuring the maintenance of both, confidentiality and integrity of data. However, the widespread use of cryptography raises a number of important issues. Governments, for instance, have wide-ranging responsibilities, several of which are specifically implicated in the use of cryptography. These responsibilities include, but are not limited to:

(1) protecting citizens' right for privacy,
(2) facilitating information and communication systems' security;
(3) supporting economic activities, by, for example, promoting electronic commerce;
(4) maintaining public safety;
(5) raising the necessary revenues to finance their activities; and,
(6) enabling the enforcement of laws and the protection of national security.

Although there are legitimate governmental, commercial and individual needs and uses for cryptography, it may also be used by individuals or entities for illegal activities which can affect public safety, national security, the enforcement of laws, business interests, consumer interests or privacy. Governments and international organizations, together with industry and the general public, are challenged to develop balanced policies to address these issues.

As the above would suggest, the divergent interests which can be affected by either the use or non-use of, or the failure to use cryptography, make the development of balanced cryptography policy both complex and critical. Cryptography, which traditionally has been primarily used by governments, has become widely accessible and affordable to private users in recent years. Moreover, media attention has further raised public awareness about possible benefits and risks with cryptography. This has further increased diffusion of cryptography software being used by many, while the debate about the issues outlined in this paper is continuing.

1.2.1. Secret Key Cryptography

Historically, cryptography has been used to cover secret information from unauthorized parties by encoding. As such, it is important for military and government security. Cryptography uses an algorithm to transform data in order to render it unintelligible to anyone who does not possess certain secret information (the cryptographic "key") necessary for decryption of data. Today, the increased calculation power arising from the development of digital computing makes it possible to use complex mathematical algorithms for encryption of data (Blaze, Diffie, Rivest, Schneier, Shimomura, Thompson & Wiener, 1996).

Secret or symmetric key cryptography uses one common key for the encryption and decryption of information. Although the existing encryption algorithms are very powerful, the drawback of this technique is the administration and distribution of the keys. The same key has to be provided to all communicating parties. Utilizing only one key for multiple parties does not allow for identification of the creator of an encrypted data file (no digital signatures). Also, if the information is modified or leaked, it can not be determined which of the parties possessing the key caused such an incident. The safety of the secret key approach lies in the difficulty to re-engineer the key and the encryption algorithm from the encrypted message. A typical symmetric algorithm is DES (Data Encryption Standard).
The development of information and communications technologies that allow vast quantities of data to be transmitted, copied and stored quickly and easily, has prompted a growing concern for the protection of the confidentiality of data - including personal data, government administrative records, business and financial information - and the protection of privacy. Effective and strong cryptography is an essential, if not the only, tool in a network environment for addressing these concerns. Unfortunately, as section 2 suggests, stakeholders' interests and concerns may be detrimental to each other. Accordingly, national defense and law enforcement concerns may be opposite to privacy and security issues of concern to citizens. Furthermore, reports about criminal activity with the help of cryptography have been exaggerated greatly (e.g., Denning & Baugh, 1997). Most importantly, criminals will obtain access to the best cryptography available regardless of defense and law enforcement wishes. Moreover, if similar yardsticks would be applied to telephone conversations and scrambling equipment, defense and law enforcement agencies would have to wiretap all phone conversations. The latter is currently illegal in most democratic countries unless a court order has been obtained beforehand. Finally, when asking people whether police should be able to tap into the Internet or whether cryptography should be restricted to help law enforcement, respondents are likely to agree (cf. McClosky & Brill, 1983). Gattiker and Kelley (1998) reported, however, that when subjects are asked specifically to give up part of their own privacy to enable these agencies to monitor their communication, people are very reluctant to do so. Accordingly, why should the measuring sticks for monitoring and limiting the public's ability to encrypt their communication via the Internet be treated differently than standards applied to the telephone? Paranoia may prevent us from approaching this rationally and fairly (cf. Section 2).

1.2.2. Public and Private Key Cryptography

In the mid-1970's a new development in cryptography introduced the "public“ or „asymmetric key" concept, which allows parties to exchange encrypted data without communicating a shared secret key in advance. Rather than sharing one secret key, this new design uses two mathematically related keys for each communicating party: a "public key" that is disclosed to the public and a corresponding "private key", that is kept secret (see also Appendix 1). The idea of this approach is that it is mathematically easy to generate an associated pair of keys, but that it is almost impossible to determine one key out of the other. This means that the holder of a (sufficiently long) public key is not able to calculate the private key, and thus, for example, fake a digital signature. A typical asymmetric key algorithm is RSA (named after the inventors of the public key approach Rivest, Shamir and Adelmann).

With this technique, if an individual encrypts a message with the public key, the recipient can decrypt it with the corresponding private key. Without the private key, the recipient of the message is unable to retrieve the readable information, thereby reducing the risk of having the information end up with third parties who have no „need-to-know“ or of having information being corrupted/altered.

In the above scenario, however, the user has to protect the private key very carefully because once it has ended up in the wrong party’s hands, intercepted messages can be decrypted by others without the originator or recipient of the message even being aware of this. Accordingly, public and private key cryptography is only as good as its users’ ability to protect their private key. Based on users’ sometimes sloppy security of their log-on password, one is allowed to be somewhat skeptical about how much better users will do with their private key.

1.3. Digital Signature

An important application for public key cryptography is the "digital signature", which can be used to verify the integrity of data or the authenticity of the sender of data. In this case, the private key is used to "sign" a message, while the corresponding public key is used to verify a "signed" message. Public key cryptography offers the benefits of confidential transmissions and digital signature in an open network environment in which parties do not know one another in advance. This development allows for broader applications of the cryptographic mechanism, and this - together with increases in computer power and decreases in computer price - has moved cryptography into the private sector domain.

Public key cryptography and digital signatures play an important role in developing global information infrastructures. Much of the interest in information and communications networks and technologies centers on their potential to accommodate electronic commerce; however, open networks such as the Internet present significant challenges for making enforceable electronic contracts and secure payments. Several different methods exist to sign documents electronically, varying from very simple methods (e.g., inserting a scanned image of a hand-written signature in a word processing document) to very advanced methods (e.g., using cryptography). According to the European Commission (October 1997), electronic signatures, based on „public key cryptography“, are called digital signatures and are widely considered as crucial for a variety of applications like digital signatures used

- for official communication with public institutions (e.g., calls for tender, exchange of application forms, identity documents, tax declarations, transmission of legal documents),

- for contractual relations in open networks (e.g., electronic commerce and financial transactions),

- only for identifying or authorizing purposes (i.e., in order to be certain of the identity of correspondents or their attributes, such as having the authorization to log into a computer system or accessing a restricted part of a network),

- in closed systems (Intranet), and

- for personal purposes.

Naturally, the above applications are rather extensive, and misuse or abuse of the technology is possible. Accordingly, application issues must be addressed and firms as well as governments are still grappling with these issues. Without eliminating potential fears of users concerning secure and safe use of such signatures, their use will be limited as the section below outlines.

1.3.1. Application of Digital Signatures

There is a tremendous potential for fraud in the electronic world. Transactions take place remotely, without the benefit of physical clues that permit identification, thus making impersonation easy. The ability to make perfect copies and undetectable alterations of digitized data complicates the matter. Traditionally hand-written signatures serve to determine the authenticity of an original document. In the electronic world, the concept of an "original" document is problematic, but a digital signature can verify data integrity, and provide authentication and non-repudiation functions to certify the sender of the data. If a document itself has been altered in any way after it has been "signed", the digital signature will so demonstrate. Similarly, once a document is "signed" with a cryptographic key, the digital signature provides proof that the document was "signed“ by the purported author. In turn, the sender cannot easily deny having sent the document or claim that the information has been altered during transmission (cf. OECD, 1997).

1.3.2. Legal Questions with Digital Signatures

The implementation of digital signatures as a cryptographic mechanism to support authentication and non-repudiation security services seems to offer a technical solution to a legal problem. However, it must be mentioned, that there are some legal questions that need to be addressed and, unfortunately, they are addressed differently in various countries. The following aspects are currently being discussed regarding legal concepts behind digital signatures, and requirements on form and procedures:

- Does a digital signature meet legal requirements?

- Is a digitally signed document recognized as evidence in court?

- Does a „Declaration of Intent“ have a legal value?

- Are there technical solutions to make sure that users sign a document in the version which is actually visible on their screen?

- Does a digital signature prove that a particular person actually signed a given document?

The last point especially is of some concern because conventionally, a person signs a signature by hand. In the electronic world, however, the technology would permit a third person – authorized or unauthorized – to sign a document, if this person is in possession of the private key („undisclosed delegation“).

Cryptography can also provide technical solutions for the protection of intellectual property in digital form. For example, a digital signature together with a verifiable time-stamp can give authors some control over their work by tying an electronic document to the issuer and ensuring that the document is not modified without detection. The same technology can be applied to ensuring the authenticity and integrity of documents archived electronically (OECD, 1997).

1.3.3. The Need for Action within Europe

The above sections on cryptograph and, especially, digital signatures suggest that countries have to move beyond the basic agreements made under the OECD's umbrella (OECD, 1997). Some member states of the European Union have already proceeded to develop detailed regulations for digital signatures. Germany has released a law on digital signatures (Bundesministerium fuer Bildung, Wissenschaft, Forschung und Technologie, October 8, 1997). France has adopted a new Telecommunications Act (Loi N° 90-1170, 29 December 1997) which is being criticized by various groups, including the French Parliament's Commission for Post & Telecom Public Service (CSSPPT) (Thorel, 18 December 1997). Italy adopted a law on the use of electronic documents and contracts (Council of Ministers, August 5, 1997). The UK government has launched a Public Consultation on the regulation of Trusted Third Party encryption (TTP) [uk_crypt]. The Dutch Government has created an inter-departmental task force [Staatscourant nr. 54, 18.3.97]. Denmark and Belgium are also preparing draft legislation on digital signatures. [http://www.agoraproject.org/]. The Swedish government organized a public hearing in June 1997.

Whilst the development of a clear framework is welcomed, the very divergent legal and technical approaches which have already appeared constitute a challenge. Moreover, the absence of any legal environment in some EU member states – while possibly justified – might constitute a serious barrier for communicating and doing business throughout the EU using digital signatures. This will undermine the free circulation of digital signature related products and services within the EU's domestic market, while hampering the development and expansion of electronic commerce. If e-commerce should be stimulated, then obstacles to digital signatures and free circulation of information must be of highest priority. As well, facilitating the use of digital signatures across national borders requires a common framework at the EU level. Such a framework is urgently needed and should be put in place at the latest by the year 2000 (Towards a European framework, October 8 1997).

2. STAKHEHOLDER ELIGIBILITY FOR MEDICAL DATA DISCLOSURE: A COST-BENEFIT ANALYSIS

Section 1 above discussed privacy issues as far as medical data stored in computer information systems are concerned. In order to improve such a system's confidentiality, integrity and availability, as well as privacy and security, we outlined encryption and digital

signature possibilities. As such, while encryption techniques could help in protecting the confidentiality of data and thus not infringe on patients' privacy, the lack of a comprehensive legal framework might make use of encryption more difficult or even illegal. Also, how digital signatures can be used effectively across national borders or even within countries to assure the authenticity of medical data about a patient in the emergency department is still not clear. In this section we are focusing on medical data and its disclosure to various parties, and how this relates to security and privacy of data, as well as how encryption and digital signatures may help to uphold confidentiality, integrity and availability of medical data as required.

Before we discuss which factors could influence information being disclosed to various parties or stakeholders, it is necessary to identify the stakeholders for the information about patients contained in a medical database. Unfortunately, while management literature on stakeholders is quite extensive and thorough, literature dealing with information systems has ignored the stakeholder issue so far except when dealing with introducing new technology.

2.1. Stakeholders and Medical Data Disclosure

People or parties wanting access to an individual's medical information may be looked at as stakeholders. Stakeholder theory (Freeman, 1984; Donaldson & Preston, 1995; Ulhøi, 1997) and experiences from environmental stakeholder pressure (Ulhøi & Madsen, 1998) suggest that a thoroughly performed stakeholder analysis can improve the likelihood of optimising corporate strategic initiatives. For a long time, researchers have pointed out that stakeholders' importance for managing will increase (e.g., March & Simon, 1958) and recent findings indicate that satisfying their needs continues to be a paramount issue.

Mitchell, Agle and Wood (1997) suggested that we expand our theoretical concept of stakeholder typology and distinguish stakeholders according to their power, legitimacy and urgency while grouping them into **latent**, **expectant** and **definite** stakeholders. In this paper we want to focus on expectant and definite stakeholders for the firm and its Web activities. Mitchell, Agle and Wood (1997) suggest that **expectant stakeholders** are made up of dominant stakeholders (e.g., large institutional investors, employees, key customers), dangerous stakeholders (e.g., wildcat strikers, terrorists) and dependent stakeholders (e.g., public demanding that firm reduces pollution may unite with media or government to get action). **Definite stakeholders** have power and legitimacy already, hence a large insurance firm may force the administrator of a medical database to change some of the individual identifiers. For instance, a person's gender is provided to insurers even if some medical data may not be given (e.g., information revealed by genetic tests performed on a patient).

2.2. Information Content

Expectant and definite stakeholders, as well as latent ones, may have divergent and often conflicting interests. These must be balanced against each other to avoid conflicts and privacy violations. Patients are a general practitioner's expectant stakeholders and dominant at that. For the patient, the doctor-patient privilege is probably sacred. Hence, the doctor is as much interested in keeping a patient's health record private as the latter since the patient may complain and possibly sue the doctor if he or she fails to use the necessary safety and security procedures to protect health record confidentiality, integrity and availability. However, neither doctor nor patient are sharing the information alone. Instead, information about prescriptions for drugs, treatments and referrals are all digitally stored and used by various parties (e.g., pharmacist, insurance company or government, if

national health care program for payment). The likelihood that information will be improperly disclosed depends on three things as outlined in Table 2.

Insert Table 2 about here

Stakeholders can obtain legitimate or illegitimate access to medical data (cf. Table 2). In computer security models, people are considered to be intangible assets, whereby their motivation and capabilities must be considered as well. Accordingly, regardless of the value of information and how many stakeholders get access to it, the number of illegitimate accesses must be reduced to an acceptable minimum. Most importantly, users must be motivated and skilled enough to follow procedures and apply offered security techniques vigorously, thereby reducing the availability of data to unauthorized users while upholding confidentiality and integrity as much as possible (cf. Table 1).

The greater the detail about a patient's every treatment, drug, change in condition and medical history back to birth in a database, the more valuable such information will be for health care providers. While the value of such information to one's physician for making better decisions about health services is high (see also Table 4 for an approach for calculating information value), other stakeholders might also consider such information to be valuable and thus demand access. At the same time, health authorities and medical personnel elsewhere might need access to such data as well, in order to reduce inadequate or even harmful treatment, while reducing costly duplication and waste of public funds (e.g., Striking the right balance, December 5 1996). Accordingly, the dilemma is that the more complete the database, the greater the number of people and agencies requiring access. In turn, the threat to patients' privacy is increased whenever the number of stakeholders and people wanting access to the data increases.

Insert Figure 1 about here

Figure 1 illustrates this dilemma graphically. Privacy is especially important when many parties obtain access to medical information such as patient records, while the value of such information for their work is high (see Table 3). Which Quadrant might fit a situation best is also affected by the factors outlined in Table 3. Even using encryption is of limited help if too many unauthorized parties see the information on a terminal or desk when it is decrypted (e.g., printed out).

Insert Table 3 about here

Before further discussing Figure 1, we should point out that, in the end, it must be the patient who determines which medical information the team providing care gets access to. Moreover, the patient must be given the opportunity to object or request that the complete medical record, or parts thereof, is restricted to one or more named clinicians. Accordingly, any large medical database being accessed by public agencies, insurers and clinicians is unlikely to have complete data if the patient has any say. For instance, the person may not want his or her medical records from prison (e.g., indicating extensive psychological counseling helping patient deal with depression symptoms) to become part of the database. The record may contain discrete flags indicating to clinicians and others that part of the

patient's medical history is hidden, and lead a clinician to ask the patient if he or she has omitted any information which might be important. Naturally, a health insurance company may misinterpret discrete flags indicating missing information.

Limiting access for various stakeholders either outright (e.g., insurers only get data without personal identifiers) or partially (e.g., flags indicating to clinicians, but not others, that some data are missing due to patient's request) will result in extensive lobbying efforts to change such laws. Excluded groups or those with limited access (e.g., insurers) will want to obtain unrestricted access primarily on the basis of improving service while reducing costs which, in turn, would benefit patients. Here, the majority of patients who do not have records which might affect their quality of life (e.g., carrying no dangerous disease) might also pressure governments to open access in order to permit them to reap cost saving benefits with lower premiums. Democracy might have to protect minorities from being harmed and treated unfairly. Moreover, confidentiality of medical data is also threatened by the fact that about 10 percent of general practitioners have already experienced computer theft and thus lost patient files stored on the machine's hard-drive (Pitchford & Kay, 1995). Below we describe how the Quadrants in Figure 1 represent the various challenges faced by regulators and managers alike when trying to establish medical record systems of various sizes and depth of content.

2.2.1. Managing Access and Content: Privacy and Encryption Issues

Figure 1 assumes that a high level of privacy is consistent with high levels of encryption used, that is, neither one is independent of the other. Quadrant A in Figure 1 describes a situation whereby an individual's records for over-the-counter drugs purchased at his or her preferred pharmacy may be recorded. The value of the information may be limited except for marketing purposes, while access to it may be given only to the pharmacist using his or her database. Nevertheless, since security measures are not necessarily in place (e.g., data in database is not encrypted), privacy for clients may be low as well, since all pharmacy employees will have access to the patient's file. Transferring files between pharmacies (e.g., in case of a national organization) is likely done without using encryption.

Quadrant B may describe a situation whereby many people get access to a patient's general insurance record (e.g., information about type of insurance). The value of such information is again limited, except maybe for marketing purposes. Moreover, privacy of this information may also be low as it is unlikely that such information is submitted to any encryption mechanisms when being transferred between offices.

Quadrant C might be illustrated by a situation whereby the database provides information about gender and age of subjects; however, personal identifiers are not given for such records while the value of the information is limited except for research purposes. While many people might get access, files may, nevertheless, be transferred in encrypted form only.

Quadrant D may be the general practitioner's private database to which only he or she has access (limited access). The data's value may be limited because no data is available for the time before becoming a doctor's patient and after having chosen another doctor. Incomplete data about the person's medical life history as well as limited access (e.g., doctor and assistant only) do not, however, result in high privacy unless encryption is used.

Quadrant E could be illustrated by a situation where data about genetic test results as performed on various risk groups are being collected. In turn, information may provide insights about the person's likelihood of catching a certain disease (e.g., risk for breast cancer). Here it might be possible that a few health professionals have access to such data to assess the potential for exposure to such a disease and effects upon future generations. The information contains personal identifiers for each citizen's record. Here privacy is limited to enable health professionals to do their work, but encryption may also be weak. Once a person has gained access, all information is available since no encryption is used.

Quadrant F could be a patient's medical record, which can be accessed by the attending physician, emergency doctors and the hospital's accounting office (for billing purposes). Privacy is limited since these records must be accessible to any doctor providing emergency care in another state/province to the patient. The value of such information is great to the stakeholders getting access.

Quadrant G represents the ideal but **unrealistic** case whereby medical data is accessed by many, the value of the information is high but, most importantly, privacy is also high. Moreover, the use of sophisticated encryption mechanisms further reduces threats against privacy. For instance, this could be illustrated by aggregate medical data being used for research purposes, whereby privacy is protected by not providing a personal identifier to stakeholders gaining access to such data (e.g., government agencies and medical researchers). Moreover, data may only be stored in encrypted form, thereby limiting its usefulness unless the person has the appropriate key to decipher the data.

Quadrant H again illustrates an **unrealistic** scenario because if a patient's medical history is given in full from birth up to this date, political pressure will be very high for access by excluded stakeholders (e.g., insurers and hospital billing departments). It is likely that, ultimately, besides one's general practitioner, many of these lobbying stakeholder groups will be obtaining access. Such a comprehensive medical database providing a complete medical history of each person is of great value to many stakeholders (e.g., insurer, doctor, government and employer). One would hope that access is limited, while privacy is high, and sophisticated encryption techniques further limit the misuse of such data.

The above information does not try to be complete, but instead provides the reader with an overview of the type of medical record being accessed by various stakeholders. Here Figure 1 implies that high levels of privacy go in tandem with appropriate levels of encryption, that is, without the latter, privacy cannot be safeguarded. In summary, Figure 1 suggests that it is extremely difficult to maintain high levels of privacy if the value of information is high, as is the case with a patient's complete medical history (e.g., Quadrants H and G) (see also Table 2). In such a case pressure becomes great to provide access for many stakeholders and it will be difficult for the patient to restrict access to a few or keep certain information hidden. For instance, what can an individual do if the insurer refuses to provide life insurance if the firm does not get access to the complete file? Even if such access is restricted (e.g., as per patient's request or by law), applicants may be asked informally to provide a print out of the complete record to which they should have access themselves under any freedom of information regulation. Also, how will an individual be able to prove that data from genetic tests may have resulted in one not being hired or insured? Hence the challenges outlined in Table 3 are nearly impossible to balance to every stakeholder's satisfaction. Below we will address in more detail the privacy issue as it pertains to medical or other records, especially as far as regulation is concerned.

2.3. The Value of Information: Dealing with Access and Content Misuse from a Cost-Benefit Angle

The above section suggests that various strategies can be used to reduce threats to information content (e.g., alteration of data), factors facilitating efforts for maintaining confidentiality, integrity and availability of medical data (e.g., Tables 2 and 3) and which measures might reduce these threats (see also Figure 1). Detailed records on every treatment, drug, and change in condition of a patient provide up-to-date and reliable information. This is essential for making good decisions about health services. At the same time, health authorities and medical personnel need access to such data in order to reduce inadequate or even harmful treatment, while reducing costly duplication and waste of public funds (e.g., Striking the right balance, December 5 1996). There are numerous efforts under way to link patient records nationally and provincially/statewide by various governments such as the USA and the Province of Alberta, Canada (Gostin, Lazzarini & Flaherty, not dated;Strategic partner selected, July 14 1997). The hope is that with the help of personal identifiers, birth dates and social security/insurance numbers and/or national health numbers, a large information system can be created. In turn, it is hoped that the electronic flow, interchange and use of patient medical records between health care organizations and other parties, such as insurance firms, will be facilitated to save time and costs (e.g., Sequoia Software, October 24 1997).

Patients, doctors and health officials to mention a few parties may, however, worry about what kind of system may be needed to encourage all parties to maintain confidentiality, integrity and availability of data. In the business context it is obvious that the value of information must be calculated in order to determine which measures may be warranted to guard oneself or the system against these risks and thus financial losses. Here a cost-benefit analysis for calculating the asset value (AV) including an assessment of costs caused by IS vulnerabilities and threats compromising the medical information system must be done. Whilst the development of a thorough model for assessing risk, vulnerabilities and threats is beyond the scope of this paper (see Gattiker & WG1, 1997, for a thorough presentation of a cost-benefit approach) Table 4 outlines such an approach.

Insert Table 4 about here

Unfortunately, rarely if ever are the potential costs for security breaches calculated before the incident has occurred. Additionally, even after occurrence various parties involved in salvaging and restoring the system including users and experts rarely if ever agree on the costs and how they might be calculated. For instance, in a recent study the average cost for a security breach of networks was estimated to be between USA $1,500 - 2,000 (NCSA, 1997). Even the author of the report stated: „this cost appears to understate the total costs of the average security breach since 14.5 hours„ (NCSA, 1997, p.14) of down time was attributed on average to each security breach. Just studying the approach in Table 4 and calculating the hard and soft costs of 14.5 hours downtime suggests that security breaches result in much higher costs.

Unless we are able to provide investors and/or managers with figures about the costs and benefits of certain policies, they are unlikely to provide the funds required to implement policies and upgrade system security. In turn better measures taken against security breaches and improved end-user skills help in reducing the likelihood of threats and vulnerabilities materializing into a serious compromise of the integrity, confidentiality and availability of a medical database and resources. Table 4 makes an effort to outline how, with the help of costs, the asset value (AV) can be calculated considering various intervention strategies, such as end-user training**,** for improving system safety

Equation 4 in Table 4 is especially important. Not only are we identifying the costs for getting the damaged file or system running again (Equation 1) but we must also consider the asset value of the object (AVO). For accounting purposes we may assume that we obtain AVO after depreciating various assets and investments. Hence, AVO could be low after two years already. The strategic issue here is somewhat different, however, in that the value of the system consists of the costs and investments made to run the system. With the help of shadow pricing (i.e., prices which we would have to have paid if the system or parts thereof would have been supplied by an outside firm) a more realistic AVO can be calculated.

Table 4 outlines in some rudimentary ways a cost-benefit approach to determine the potential costs occurred by an information provider (e.g., government agency managing medical database under contract) if data confidentiality, integrity and availability (CIA) is no longer maintained (cf. Table 1). In particular it outlines a practical approach for determining the value of information stored in a medical database and possible costs incurred if CIA can no longer be maintained. For instance, a person's death might be attributed to wrongful information provided to medical personnel, resulting in the patient's heart failure. Subsequently, a liability suit against the manager of the national medical database on behalf of a now dead patient might be launched. Accordingly, maintaining satisfactory privacy, safety and security standards requires some cost-benefit analysis in order to determine which measures must be undertaken to minimise financial and social costs to an acceptable minimum. Nevertheless, to make such a financial assessment feasible and workable, access and regulatory issues must be addressed and harmonization of legislation across countries and states is needed as the following section will show.

3. SAFEGUARDING PRIVACY: ACCESS AND REGULATORY ISSUES

Any new medical information system containing centralized records from patients has to address the value and access issue as outlined in the previous section of this paper. Since information in such a database is valuable to many parties including the patient, access, encryption, digital signature and privacy issues are of paramount importance. Figure 1 suggests that a careful balancing act between stakeholder interests and needs for information from governments, insurers, employers, doctors, hospitals, pharmacists and, most importantly, patients is required to succeed as far as privacy is concerned. In turn, while the need for privacy protection of patients' records is needed, data encryption may be required to attain satisfactory privacy levels. Nevertheless, even encryption does not prevent some clever individuals or machines from breaking the code and thus deciphering data or simply stealing such data while violating somebody's privacy (Abelson et al., 1997; Blaze et al., 1997). Below we discuss these issues in some more detail.

3.1. Access to and Value of Information

Table 1 outlined how the security of an information system requires that the confidentiality, integrity and availability of data can be maintained. Figure 1 graphically illustrated what data access and its value might mean for a patient's privacy, and how encryption might be applied effectively to support the former. Tables 2 and 3 outlined some of the factors possibly threatening our efforts to maintain privacy, confidentiality, integrity and availability of data; options we have to reduce threats and vulnerabilities of databases holding important medical information were also sketched out. Finally, Table 4 presented a cost-benefit approach to determine which measures should be undertaken to minimise social and economic costs when privacy is being violated.

While Figure 1 did not address the legitimate or illegitimate use of data, it illustrated graphically how difficult it is to balance access and value of information while using encryption in order to strengthen privacy satisfactorily. At this stage, most efforts for medical databases sponsored by governments indicate that the latter intend to collect as much data as they can in order to facilitate the use of accurate and complete information by health care professionals (e.g., Government introduces draft, June 11 1997). However, the greater the completeness of such records, the greater the value of the information they contain to various stakeholder groups (see also Table 4). Accordingly, the potential threat by parties wanting illegitimate access increases. Moreover, the threat to confidentiality, integrity and availability of data stored and maintained with such a system - containing information about several millions of users - is substantial (e.g., through natural disasters).

Whilst access to such information can in theory be limited to physicians, numerous other people will get access. For instance, in an emergency ward nurses and even orderlies may obtain access to vital information to save somebody's life by using their personal password to speed up health care services provided to the patient.

Naturally, strong identification and authentication measures can be used. For instance, biometrics such as touch pad (for checking genetic fingerprints), voice, body's low current and others may help in forcing people to access the data personally, instead of „authorizing" somebody else to do so on their behalf. But still, in an emergency the doctor may provide the biometrics information needed to gain access to the database. However, subsequently, the attending physician might be asking the attending resident to search the database and obtain the information required, while the doctor is taking care of the patient at the same time (i.e., division of labor). Moreover, sensitive information from a national cancer database has been known to be stored in garbage bins outside the facility over the weekend before being collected and subsequently destroyed (Harley, 1998).

It should be made clear that the above described scenario is a description of a „day-in day-out" situation, and that the implementation of a verified security policy based on a solid theoretical mode would not permit such a situation to occur. The problem is the difference between theory and practice where, under certain emergency situations, people resort to measures helping them accomplish their job objectives more quickly, while endangering the confidentiality, integrity and availability of a database and possibly violating a patient's privacy. Here, attribution of record access (e.g., who, when, what and where/location) may not be very helpful as audit trail in trying to close a leak. For instance, 12 people may have looked at a print out of the file, and the janitor may have collected it from the trash and sold it to an interested illegitimate party. Many more such scenarios can be imagined and are possible. In real life, 100 percent accuracy rates are just theoretical and nearly impossible to achieve.

The above illustrates that biometrics might, in theory at least, help in restricting access to very valuable medical information to parties which really require such information to provide patients with effective and cost efficient health care. Unfortunately, in practice, factors may undermine the use of biometrics and its effectiveness. Additionally, this method may be cumbersome and costly to administer (e.g., keeping biomedical data records for rapid on-line verification around the country). Moreover, this approach would not prevent that some parties might misuse their well-intended privilege for getting access to data with the intent to pass information on to other interested but unauthorized parties (e.g., names of HIV patients). Again, technology is only as good as the humans taking advantage of it; this applies to medical information and its disclosure from a database as well.

3.1.1. Using Health Cards: Problems Remain

In Germany, by law, all persons insured in the mandatory public health insurance system are provided with a chipcard containing their insurance data. For now the card contains only administrative data, like the person's name, gender and insurance number. For instance, in Denmark the card number is made up of the person's birth date. One idea is to also store medical data on this card. In turn, this would improve transportability of these data between various health care institutions. The privacy risk is obvious. Encryption could support privacy, for example, by creating three data domains on the card:

1. Public: This domain contains administrative data about the person, as it is already nowadays available. No or only very weak encryption (basically to ensure integrity) is needed.

2. Private: This domain should contain more or less the subject's full medical records (probably including hyperlinks to centralized databases containing X-ray pictures etc.). This domain needs strong encryption and a password system, which allows only access by the patient (Read-only), and a trusted medical party (e.g. personal physician) who can add data and updates. For these updates the combination of the patient's and the personal physician's key would be required, thus providing for traceability of changes.

3. Emergency: This domain contains data readable by emergency and medical services using a general key to access such data. This domain would only contain limited data such as a person's diabetes, cardiac problems, blood group and allergies against drugs. For data updates the same provisions as for the private domain would apply.

The above example would reduce some of the threats inherent in any huge database with records at least at first glance. Nevertheless, to assure integrity and availability of such information, backup procedures would be needed. For instance, if the individual looses the card or it somehow becomes damaged, a centralized database would have to be used to re-issue a card. Hence, the usual threats and risks against confidentiality, integrity and availability of data apply to this centralized database (cf. Anderson, 1996). Moreover, various stakeholder groups will continue pressuring legislators to get access to the information on the patient's health card (e.g., insurer requires annual updates).

The above illustrates that while the German approach, as well as Denmark's if pursued further, might reduce threats to privacy of patient data, but that in the long term the challenges will be the same as for a centralized data-base as those considered in the USA, UK and some provinces in Canada.

3.2. Legislation and Privacy

Safeguarding of privacy does in part depend on who gets access, and the value attached to the information. Accordingly, as pointed out before, the more people have access to information and the more valuable it is for various stakeholders, the more likely certain parties will be to offer a reward for purchasing such information illegitimately (see also Figure 1). Governments have been trying to respond to this challenge by undertaking legislative efforts in national and international forums to further protect privacy. Moreover, while geographical boundaries are removed with new information technology, governments are just starting to grapple with legal and other issues (see also Section 1.3.3. The Need for Action within Europe).

3.2.1. Regulation and Sharing of Data

Many governments are trying to create national or regional databases with their citizens' health care records (e.g., Alberta, Canada and the USA Federal Government for Medicare). The attempts undertaken by the Province of Alberta in Canada to create a province-wide medical database will increase the information available to health-care professionals in the Province. It might even possibly help in lowering costs for health care delivery. However, how data exchange between provinces/states and countries may by handled by the proposed health information system is not addressed in any publicly available document. It must be mentioned here, that such a central database would be the focal point of threat and thus increase the associated risks substantially (e.g., Government introduces draft, June 11 1997 and Strategic partner selected, July 14 1997). Accordingly, would Alberta be able to share its data about one of its citizens with another province's health information system in the case of a person moving to or from another province? What about sharing data with the federal government, with or without personal identifiers, for health care policy measure purposes? How would privacy concerns be regulated if access to data were given to parties subject to different privacy legislation (e.g., in two provinces/states)? What about one of its citizens having an accident in the USA or Europe and getting treatment there? Would physicians located abroad get access to such information and if so, how? How will treatment information from abroad be added to the database to assure its completeness? For instance, USA or European laws may prevent a physician providing information about treatment given to an Albertan to a database in Canada.

Besides the challenges for governments as far as legislation and the use of health information by agencies in different provinces/states are concerned, insurance companies providing health care or supplemental health insurance (e.g., for prescription drugs) may demand access to such a database in order to offer lower rates. If such a firm obtains access (partial or complete), can or should it be prevented from using this information when offering life, car and theft insurance to clients? For instance, information from a person's medical data-file can legitimately or illegitimately be used when considering an individual for car insurance (e.g., person receives drug against seizure, should rate be adjusted accordingly?).

Legislation may prevent a firm from using health information from one of its clients for other purposes (e.g., when applying for another insurance). However, insurance firms will lobby against such legislation with the argument that by being prevented from using a fully integrated database for each customer, huge cost savings cannot be realized. Not having a fully integrated customer data base will increase privacy for clients while reducing the threat against confidentiality of their medical data. Unfortunately, as this example shows, privacy does not come for free. More privacy means less integrated medical and customer databases with limited access to those only as stipulated by the individual. In turn, cost savings for governments and firms will be limited. Unless some legislation is put into force, privacy protection becomes a financial issue; that is, individuals with the necessary wealth will be able to afford higher insurance rates due to not providing medical records to insurance firms.

3.2.2. Legislation for Public and Private Data

Another problem with a publicly sponsored medical information system is that legislation for public servants and employees from private organizations may differ as far as privacy of medical information is concerned. For instance, Québec has had privacy protection for quite some time on how public organizations were supposed to handle data from and about citizens. In contrast, how private firms are supposed to protect customers' privacy was not really addressed until a bill was put into force in 1993 (Bill 68 1993, Chap. 17; August 4,

1993). Often we have a privacy law for public but not private data, that is, while privacy policies may apply to public agencies, business' and others' use of data may experience limited if any regulation in some countries. Moreover, medical data and privacy have been addressed, but it is not always obvious how general privacy laws for governments and/or private business apply to medical data (e.g., HIV information). Here a firm or doctor may experience a dilemma in cases where one might serve several masters. For instance, the doctor–patient privilege might be threatened if a test is requested on a prospective employer's request. While the HIV data may not be accessible normally, the personal physician may know about this. Can the physician invoke the doctor--patient privilege and thus not report this information to the prospective employer who is paying for the medical tests and the report? Moreover, what will the employer do with such a report and its information (e.g., will it be destroyed immediately or put into the new employee's personnel file) (see also Information Policy Committee, April 1997 for an extensive discussion of this issue)?

As outlined in Section 1.1.1, freedom of information is also an important issue here. For instance, is the individual given permission to restrict access to one's medical file by a government agency (e.g., police) for other uses? To illustrate, at a speed checkpoint police may appreciate having access to a driver's medical data file about his or her possible addiction to a substance and medical or psychiatric treatment against it. In contrast the individual may not want the agency to have this information available when erratic driving due to a small seizure leads to an accident. Today, most countries do not provide an individual with access to police files to check for accuracy of the information. If one has a suspicion, a data privacy commissioner may examine the files on the citizen's behalf. A taxpayer may also claim a deduction for medical expenses when doing annual filing for taxes. In turn, tax authorities might wish to check such a claim against one's medical file, thereby reducing possible fraud and the costs to determine legitimacy of such deductions. Should this be possible and if not, how can the individual check or protect his or her right? Today, most countries only provide citizens with limited recourse against various government agencies exchanging data and collaborating for performing their tasks more efficiently. In turn, the number of people getting access is raised substantially, while keeping data confidential is further reduced. Privacy may be impossible to maintain at a satisfactory level unless huge databases with extensive individual records are not created (see Table 3).

3.2.3. National and International Issues

As the above suggests, even as far as domestic regulations are concerned, not everything is rosy. Additionally, large organizations doing business in the medical/health care field, as well as in other areas will face a difficult challenge and possibly dilemma trying to satisfy privacy and business demands when using medical databases. In addition, globalization of trade puts another twist on privacy issues for business and governments.

The Québec law (Bill 68) was this province's response to European Union (EU) legislative efforts and regulations first released to the public in 1991 (Directive of the European Parliament and the Council, adopted by the Council July 24, 1995). The EU directive forced member states to adjust their national privacy legislation to meet EU regulations by October 1998. Countries such as Holland and Sweden have already adjusted their national legislation to meet EU regulations, while others such as Germany and Italy are in the process of doing so. Since the EU directive came into force on October 1, 1998, EU privacy regulation has affected data transfer and information exchange between organizations in the EU and others outside its borders. Hence, Québec wanted to make sure that its legislation would enable Québec firms to receive and exchange customer and other data

with subsidiaries and other firms located in the EU. Many firms located in Ontario have adjusted to meet Québec guidelines and, in turn, most firms doing business across provincial borders in Canada follow Québec 's Bill 68 when dealing with data privacy.

The above illustrates that while official negotiations for harmonization between privacy legislation in Canada and the EU may have been lacking, Québec's efforts have resulted in some informal harmonization between Canada and the EU by bringing their legislation in line with each other. The biggest obstacle for Canada, the U.S. and the EU is how data exchange will be affected in the future. It would be reasonable to assume that a legitimate transfer or exchange of medical information from a database in the EU to the USA or Canada by an insurance firm would not be possible because the latter two's privacy legislations do not meet EU standards. In turn, large insurance companies wanting to outsource their data entry and processing work and/or centralizing their databases to achieve cost reductions and raise efficiency will experience some difficulty in doing so. Here, trans-national negotiations resulting in further harmonization of domestic laws with international ones will be needed to permit firms to centralize their databases with customer and other important data.

3.3. Regulation of Encryption

As the above shows, data legislation for private organizations in addition to public ones still needs effort in most countries, provinces and states. Worse, however, is that even though globalization is becoming ever more prevalent in most business sectors, harmonization of privacy and security laws is lacking. In contrast, an international organization is able to handle disputes in the trading domain quite successfully (e.g., World Trade Organisation = WTO).

As outlined in Section 1 and Table 1, confidentiality and integrity of data are facilitated if encryption technology is applied, thus increasing privacy of data being exchanged legitimately between two parties (cf. Figure 1). In this section we will discuss how encryption policies and legislation may facilitate or hinder organizations' efforts in protecting privacy of their client data.

3.3.1. Export Control Measures

Concerns over foreign threats to national security have been the primary motive for export controls. Whilst countries want to protect their own military and diplomatic communication through encryption, the objective of export control is precisely to deny similar benefits of cryptography to foreign opponents. Therefore, export controls are in general designed to prevent international proliferation of certain encryption technologies.

Under the *Wassenaar arrangement on export controls for conventional arms and dual-use goods and technologies* (The Wassenaar arrangement, December 20 1995), replacing the Co-ordinating Committee for Multilateral Export Controls (COCOM), a group of 28 countries applies export controls to encryption products.

Within the European Union, the *Dual-Use Regulation* (December 1994) establishes a common framework for exports of dual-use goods (Council Regulation (EC) 3381/94, December 19, 1994). This regulation sets up a community regime for the control of exports of dual-use goods (i.e., civil and defense applications) by establishing a list of goods covered by the regulation. Accordingly, certain encryption products may only be exported on the basis of an authorization. In order to establish an internal market for dual-use goods, such export authorizations are valid throughout the EU.

Moreover, according to Article 19 of this Dual-Use Regulation, member states exercise a license procedure for a transitional period and for intra-community trade of certain particularly sensitive products. For the time being, this also includes encryption products. This means the regulation obliges member states to impose not only export controls (i.e., controls on goods leaving Community territory) on dual-use goods, but also intra-community controls on cryptography products shipped from one member state to another.

This Dual Use Regulation, however, does not fully specify the scope, content and implementation practices of national controls. Consequently, a large variety of domestic licensing schemes and practices exists. Divergence between domestic and EU regulations as well as others can lead to distortion of competition.

3.3.2. Domestic Control Measures

Law enforcement authorities and national security agencies are concerned that widespread use of encrypted communication will diminish their capacity to fight against crime or prevent criminal and terrorist activities. For this reason, in several EU member states, consideration is being given to how their encryption policy could develop in the future. This has led to national and international discussions about the need, technical possibilities, effectiveness, proportionality and privacy implications of such a regulation.

3.3.3. Existing Regulation within the European Union and the OECD

Whilst export control measures are internationally widely applied, up to now, domestic control of encryption is quite exceptional. In fact, currently only one member state of the European Union, France, applies a comprehensive cryptographic regulation. The Prime Minister (in practice the SCSSI which stands for „Service Central de la Sécurité des Systèmes d'Information“) submits provision, export and use of cryptography to a simple declaration that the cryptography can have no other object than authenticating parties or ensuring the integrity of information, otherwise it must have prior authorization. This law is currently being modified (Loi N° 90-1170, 29 December 1997). Although there have been discussions in other member states, only the United Kingdom has so far launched a Public Consultation on the regulation of TTPs for the provision of encryption services (but not for use of encryption (DTI, 1997)).

The international picture is quite similar. Looking at the OECD countries, besides export controls, there are basically no domestic regulations implemented. In the USA - where up to now no domestic regulation is in place - there is an intensive debate on several legislative initiatives. In taking up the developing debate on this topic in some OECD member countries and trying to avoid obstacles to international trade and commerce resulting from divergent national policies, the OECD has adopted guidelines for a cryptography policy.

3.3.4. Regulation about Use of Encryption

Regulation of use would mean to rule the use of encryption without an authorization as illegal. Alternatively or additionally, supply and import of encryption products and services could be brought under an authorization scheme. Authorizations would either be denied or granted under certain conditions, for instance, to use only weak encryption or to sell only approved software. These conditions are scaleable to satisfy any perceived needs of law enforcement and national security agencies.

Such regulations could limit the use of encryption. In addition, divergence between regulatory schemes might result in obstacles to the functioning of the Internal Market, in particular for free circulation. If an encryption software company, which can freely develop its products in its home country, must comply with specific technical or legal requirements in other member states, this company has to produce at least two, if not more, different versions of its encryption software. The same situation occurs if enterprises want to offer cross-border encryption services.

Today, nobody can be totally prevented from encrypting data, especially criminals or terrorists who can use encryption for their activities, for three reasons:

1) Access to encryption software is relatively easy, for instance by simply downloading it from the Internet.

2) It is difficult to prove beyond reasonable doubt that an accused has sent an encrypted message without prior authorization. Electronic communication on open networks is not like an end-to-end telephone conversation, where people can be identified by, for instance, their voice, and

3) Encryption is also possible using steganographic methods. These methods allow one to hide a messaging other data (e.g. images) in such a way that even the existence of a secret message and thus the use of encryption cannot necessarily be detected.

As a result, restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks. It would not however totally prevent criminals from using encryption. Most of the few criminal encryption cases that are known and used for justifying governmental regulation of encryption concern „professional“ criminals or terrorists. However, it is unlikely that such parties would be stopped from using this technology even if regulations would prohibit them from doing so (cf. Denning & Baugh, 1997).

Some agencies have suggested the use of TTPE (see Appendix 1 for a definition of the term) to reduce misuse of encryption. The purpose of TTPE systems is to preserve the ability of the intelligence and law enforcement agencies to access and decrypt information if necessary to fight crime and terrorism. With the help of TTP, procedures for disclosure to such agencies of encryption keys are established. However, such an approach faces two major challenges:

> (1) the sheer volume of keys to be stored over time assuming a wide use of encryption technology by consumers, medical and other organizations as well as governments;
>
> (2) trans-national concerns whereby a person or organization’s communication is decrypted in another country by a law enforcement agency that would not have been given these keys under a more democratic regime (e.g., unless court order was provided).

Public key infrastructures will probably result in a nightmare for private and corporate users worldwide with substantial costs to be paid by users and misuse and abuse by unauthorized parties being an ever possible threat. Current discussions in France about legislative efforts for public encryption do not suggest a practical solution to this problem (e.g., http://www.freenix.fr/netizen/chiffre/advice-ce.html).

4. IMPLICATIONS AND CONCLUSION

Comprehensive medical record keeping and the beginning of intelligent computer-based agents that can exploit patient records mark the beginning for, hopefully, further improving the quality and/or reducing the costs of health care for governments and people. Unfortunately, as this paper outlined for the reader, side effects such as privacy losses and misuse of information, as well as possible technical and social problems to data and information confidentiality, integrity and availability are numerous.

This paper discussed both technical and social issues as far as encryption and privacy of medical records are concerned. Specifically, how divergent stakeholder groups' interests might result in conflicts and how this could affect our possible success in limiting health care costs with the help of medical databases was outlined. Furthermore, how local and international regulation, or lack thereof, may further hamper the implementation of medical databases and their effective use in providing health care was discussed.

The issues covered in this paper have implications for any large database used by organizations and governments around the world. Accordingly, while we focused primarily on medical databases, customer, supplier and investor/broker databases require the addressing of the same issues (e.g., technical, social and regulatory) as far as privacy of such data are concerned. Below we discuss practical implications in some more detail.

4.1. Implications for Security Professionals

This paper indicates that security professionals are faced with many challenges as far as privacy, encryption and security of databases are concerned. The increasing use of public networks offers the possibility for more and new business, creating new channels of distribution and new methods of reaching the customer. However, the noticed threats and vulnerabilities to information management using technology currently threaten the realization of such information opportunities. Additionally, confidentiality, integrity and availability of databases must be questioned, while privacy for citizens and consumers is threatened. As outlined in this paper, these factors pose a risk to information for security professionals trying to implement and safeguard such information systems.

At this stage, the risks outlined here must be countered effectively; however, this seems to be the greatest challenge for all stakeholders (e.g., patients, doctors, regulators, information systems specialists and others). Insufficient or non-existing laws or regulations are currently the biggest impediment to the implementation of available state of the art technology. Such technology is withheld from the public-at-large by a small group of stakeholders (i.e., security and defense establishments), claiming that they do it to protect society.

Security professionals who are confronted with these problems should join initiatives that support the protection of privacy and the free availability of strong encryption technology. Security professionals should help these initiatives and citizens action committees in finding arguments, which, in turn, convince members of parliament to support legislation and regulation that are truly based on real users' requirements. Unfortunately, legislation and regulation is often based on proxy statements from intelligence or law enforcement forces, while legislators' understanding of these issues is stretched beyond comprehension and understanding of intended and unintended effects.

From the technology side of the coin, it is paramount that security professionals do understand that public key cryptography is not about confidentiality protection, it is primarily for digital signatures and the trusted distribution of keys. However, the principle of trust is only working as long as no third party is involved in the process. Neither does the involvement of a third party make sense from a business perspective since administration of many keys is a nightmare and would be extremely costly. In other words: How many third parties would you trust?

4.2. Implications for Public Policy Makers

The short review of regulatory developments as presented here does not provide the reader with a comprehensive review of the many issues involved. Nevertheless, the overview indicates that regulatory efforts are still lagging behind the technical developments of e-commerce and use of the Internet for communication purposes. Worse is probably that international harmonization is non-existent for all practical purposes.

International treaties, constitutions and laws guarantee the fundamental right to privacy (e.g., Privacy International, 1996). Treaties, constitutions and laws guarantee the communicating parties the right to secrecy of such communications (e.g., European Commission, Telecommunications, Information Market and Exploitation of Research, October 1997; Towards a European framework, October 8 1997). The debate on the free availability of strong encryption technology (or the limitation of it) directly affects the individual right for the protection of privacy and the requirements for data protection for electronic commerce.

Strong encryption technology without key escrow or key recovery offers fundamental protection to those who seek to bring official abuses of power to light. Any restrictions on use of encryption would create opportunities for the violation of free expression for individuals in countries where dissent is punished. Dissidents and human rights organizations under repressive regimes use encryption technologies to share their concerns and transmit information which is often sensitive. Encryption has the power to authenticate the identity of these authors to their partners abroad, and protect their identity from despots at home. Any key escrow mechanism will result in loss of confidence among groups and individuals, mostly based in repressive regimes. This would mean a tremendous blow to international efforts to support the cause of human rights (Akdeniz, 1998).

4.3. Implications for End-Users and Consumers

For end-users and consumers or patients, the picture is not very rosy either. It will be difficult to convince legislators, politicians and organizational interests (e.g., insurers and health care managers) to abandon their ideas for national information systems about citizens and their respective health data. The realization of such a huge database may ultimately violate people's privacy or at least invade it necessarily (to save their life) or unnecessarily (e.g., data about venereal diseases ends up in the local newspaper). Worst of all, if non-authorized parties obtain such data, criminal activities may be the result (e.g., extortion from some citizens by some groups based on information obtained from their medical records).

Regulators have been concerned about illegal use of encryption technology by a very small group of people who will use the best technology regardless of what regulators might have put on the books. Nevertheless, politicians striving for containing health care costs by using information technology may have been too pre-occupied with technology matters, thereby forgetting that the most obvious approach of charging user fees may result in much bigger

gains. Accordingly, user fees will reduce unnecessary doctor visits, while different health care charges for non-smokers and people who exercise regularly may result in huge economic savings well beyond the few million dollars saved with information technology. Naturally, user fees should not apply to certain groups to assure doctor visits where needed (e.g., for children and people on welfare). More importantly, such a policy will likely improve the quality of life for many while restricting medical information to the caregivers that need such information. In turn, people's privacy will be far better protected than it will ever be if we implement national health care databases.

For citizens and consumers, the challenge will be to make their concerns heard by legislators and interest groups (e.g., industry) alike. Unless action committees and voters start lobbying their parliament representatives now and put privacy, encryption and health information disclosure issues at the top of legislative agendas, they will ultimately be faced with an environment not reflecting their wishes, needs and desires. Leaving such issues to politicians and various stakeholder groups, including lobbyists, will come to haunt consumers and citizens in the future. Accordingly, this may be the last opportunity to change the direction of a running train not following democratic principles nor adhering to the wishes of majority.

4.4. Implications for Researchers

For researcher, the issues discussed in this paper suggest that some additional empirical as well as theoretical work is required to improve our understanding about privacy and encryption. Ultimately this should be helping policy makers and the public to put those policies into place facilitating e-commerce for the benefit of all while strengthening privacy and security. End-user computing needs to address quickly what policies and procedures must be used to assure that confidentiality, integrity and availability of medical data is assured while threats by users not adhering to policies most strictly is minimized.

At this stage, policies and regulations may be put in place which fail to take into consideration human behavior and, as importantly, cultural differences when comparing users from numerous countries. This will require some more understanding about users attitudes and behaviors when using databases and the Internet in general. Most individuals may be more concerned about the price of oranges or bananas at the local supermarket, than security of computers and how lack of encryption and computer viruses may hamper privacy of their medical data.

While the basics of trust framework are changing, many trust models are in existence. Researchers should also investigate the practicality of a certificate revocation list (CRL) for digital signatures, considering appropriate mechanisms for millions of certificates. Moreover, we lack an understanding of what type of management structure can help in facilitating CRL and encryption key management. Finally, multiple levels of trust may be used and researchers should investigate which one's may be used for what type of data (e.g., medical versus shopping data).

4.5. Conclusion

While information professionals and researchers wrote this paper, our conclusions would indicate that we are not necessarily willing to run down a dead-end alley. While we believe in the advantages of information technology, we are afraid that its unwise application with national health information systems without considering regulatory implications (nationally and internationally) while leaving human behavior and interests out of the equation, is politely put, dangerous if not outright negligent and irresponsible.

As Table 4 suggests managing threats and vulnerabilities against a medical database as well as maintaining, confidentiality, integrity and availability requires that costs are calculated carefully in order to assess which responsibilities by system personnel and others have which ranking on the priority list. In turn it may happen that certain threats are treated more lightly than others, simply because the probability of such a threat ever occurring, as well as the costs if it does, do not justify huge efforts and/or investments to reduce the threat or vulnerability. However, some threats (e.g., alterations of information or wrongful entry) may ultimately threaten a person's life and well-being and thus become a social and ethical issue in us deciding what values and costs must be attached (e.g., compensation to patient or one's dependents).

While legal frameworks are inconsistent and fragmented, we need to achieve compatability of laws across nations. Moreover, the lack of definition and insufficient scope of current laws must be improved upon. We urge all parties to carefully balance economic, political, and individual concerns, as well as ethical and moral issues about safety, security, privacy and economic concerns when discussing the feasibility of large-scale medical databases. The concerns outlined here might overshadow any small economic benefits that might be gained through such information systems. Thus it is each reader's responsibility to protect and secure privacy and confidentiality issues by advancing these issues and insisting on the right of each citizen to encrypt his or her communication without third party interference.

The issues outlined in this paper will continue to be of interest to many and the reader is referred to Appendix 2 for links to interesting sites for keeping abreast new developments. Finally, there has been a long line of severely deficient medical privacy bills in the USA congress of which some would result in an individual having to provide authorization to health plans, employers, and providers to decide how patient information can be used and disclosed. Only such authorization would make health care coverage possible while law enforcement officers accidentally violating the law by divulging information about a person's medical records may not even be liable (see Senator Jeffords introduced S. 1921, Health care personal information nondisclosure act of 1998). Technical limitations already may threaten privacy. Senator Jeffords' proposed bill would permit privacy violations from the start without giving a patient much recourse. Not much to look forward to or is Orwell just around the corner?

Appendix 1

Key Terms Used in this Paper

Cryptography	Is the science of keeping a message secret.
Encryption	Encoding of message contents thereby hiding the data/information from outsiders, in turn, the encrypted message is called ciphertext.
Decryption	Denotes the process of retrieving the plain text from the ciphertext.
Algorithms	All modern algorithms use a key to control encryption and decryption
Symmetric (or Secret-key)	Uses the same key for encryption & decryption, or the latter key is easily derived from the encryption key
Asymmetric (or Public key)	A different key is used for encrypting and decrypting a message; accordingly, the decrypting key cannot be derived from the encrypting key.
Digital Signatures	Public-key algorithms can be used to generate a digital signature, which is a block of data used to create some authentication.
Public key	The public key is used to verify that the signature was really generated using the corresponding private key. Public keys are often registered with a third party and can be downloaded so the person can check if the key is genuine.
Private key	The party initiating the sending of the document with the signature generated generated this key; it is needed to generate the digital signature.
Privacy	Could be defined as the individual's right to *determine* his or her own *communication contacts* and the right to *control the use of personal information by others* (Gattiker, Kelb, Janz, Holsten, Greshake, Schwenteck, & Miller, 1997 p. 606). Additionally, it should be made *technically and economically feasible* for the *individua*l and for commercial *organisations to control and protect their own private data* to an extent that *they determine themselves* and, as importantly, with *measures selected at their own discretion*
Key Recovery (sometimes called Key Escrow)	Provides some form of access to plain text outside the normal channel of encryption or decryption for a third party such as a law enforcement agency.
Trusted Third Party Encryption (TTPE)	Private keys are either stored with a public or private agency acting in a trust capacity. The existence of a highly sensitive secret key or collection of many keys must be secured for an extended period of time.
Tempest	Transient Electro Magnetic Pulse Emanation Standards which, if implemented on a particular hardware, prevent a party to do data snooping without the harmed party being aware of its privacy being violated.
Pretty Good Privacy (PGP)	A software package permitting users to use encryption when exchanging messages, widely available. Export versions of PGP are different than versions used in the USA and Canada.
PMI	Provider of medical information; could be a firm doing this job on behalf of the government or a government agency/department providing the service.

Note. When developing this Appendix we benefited from work by others ("Cryptographic algorithms," not dated*).*

Appendix 2

Interesting Safety/Security/Privacy and Cryptography Sites

http://security.WebUrb.dk
http://www.eicar.org
http://tim.weburb.dk/index.php3?src=13

We did not attempt to be complete when compyling the list below.

How to Develop Effective Privacy, Security and Access Policies

Direct Marketing Association - USA http://www.the-dma.org/policy.html

Allows you to develop a privacy policy on-line to be displayed on your Web site for free.

Privacy Policy for Corporate Use – Canada http://www.TIM-Research.com/information/privacy.htm

Privacy policy developed based on research and used in several organizations around the world. The policy incorporates latest European Union directives as well as Québec legislation, both considered the most restrictive/protective ones worldwide.

National Computer Security Association Hotlinks - USA http://www.ncsa.com/hotlinks/

Offers links to security/safety/virus sites according to various categories.

Access Policy - USA http://www.on.com

Provides a sample access policy. Links to several other sites where successfully implemented access policies are also listed.

Privacy Related Sites

Anonymizer http://www.anonymizer.com/

If you want to surf the web anonymously. But does it really work?

Digital Citizens Foundation - Netherlands http://www.db.nl/

Offers interesting information about privacy issues in Europe (English version available!).

Electronic Privacy Information Center- USA http://www.epic.org

Great source for privacy issues, developments, policies, etc.

Electronic Frontier Foundation - USA http://www.eff.org

The objective as stated on the Web page is: „The Electronic Frontier Foundation is a non-profit civil liberties organization working in the public interest to protect privacy, free expression, and access to public resources and information online, as well as to promote responsibility in new media.“

Electronic Frontier Foundation - Canada http://insight.dcss.mcmaster.ca/org/efc/

This site has a more international focus on privacy, security and legal issues than the one in the USA.

European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html

The EU directive establishes European-wide privacy standards for the processing of personal information and has raised questions about the adequacy of privacy laws in the US.

Framework for Global Electronic Commerce – Privacy - USA http://www.iitf.nist.gov/eleccomm/ecomm.htm#privacy

This is the key USA administration document on electronic commerce and privacy

OECD Guidelines on Protection of Privacy and Transborder Data Flow http://www.oecd.org/dsti/sti/it/secur/prod/

A set of international guidelines adopted in 1980 that form the basis of many national privacy laws and many voluntary codes of conduct

Options for Promoting Privacy on the National Information Infrastructure - USA http://www.iitf.nist.gov/ipc/privacy.htm

Extensive review of privacy options prepared by the National Information Infrastructure Task Force in the USA.

Privacy and the NII: Safeguarding Telecommunications Related Personal Information – USA http://www.ntia.doc.gov/ntiahome/privwhitepaper.html

NTIA white paper on privacy issues

The Protection of Personal Information: Building Canada's Information Economy and Society - Canada http://strategis.ic.gc.ca/privacy/

A recent consultation document on privacy from the Canadian government

TIM-Research Virtual Research Organisation –Canada, Denmark, Germany, Singapore http://Research.WebUrb.org

Other pointers about privacy, security, hackers and much more to various sites around the world including to research papers.

Cryptography Related Sites

ASCOM PGP and Cryptography
Page - Switzerland http://www.ascom.ch/Web/systec/
IDEA encryption http://www.ascom.ch/Web/systec/security/idea.htm
Of interest with many links is also http://www.ascom.ch/Web/systec/security/crypto.htm

Presents information about the IDEA encryption technology which is not hampered by USA export restrictions, i.e., non USA. technology, used in latest Pretty Good Privacy (PGP) software Pages load slowly during Swiss business hours.

Helsinki University of Technology - Finland http://www.cs.hut.fi/ssh/crypto/
Laboratory of Information Processing Sciences

Provides interesting non-partisan information about how encryption works, what types of solutions are available including software. Documents are written so a non-technical wizard can follow the matter easily.
This site also has tons of other information about encryption and data security including very interesting links.

RSA Laboratories - USA http://www.rsa.com/rsalabs/newfaq/

So you wanted to know something about encryption and how it works. This 203 page document is a real gem and after having read it you should have a thorough understanding about this issue. The document is being updated quite regularly.

The US PGP Home Page http://www.pgp.com/
The International PGP Home Page - Norway http://www.ifi.uio.no/pgp/

PGP 5.0 (formerly known as PGP 3.0) is the latest and most current version of the Pretty Good Privacy (PGP) encryption software, free for personal use. It adds many new features not found in earlier versions, including support for other encryption algorithms than RSA and IDEA. PGP 5.0 is the first version that is fully integrated with the Windows 95/NT and Macintosh operating systems. Works with Eudora Pro 3.02 or higher. It is available for international users since August 1997 at the above site (USA and Canadian users will be connected to a North American site). Commercial versions are available but they require a license for the IDEA encryption technology (see ASCOM above).

Make sure that you don't down load a copy of PGP that is physically inside the USA if you are not in the USA or Canada (Canadian citizen) to avoid legal problems. If you down load from the above Norwegian site and you live outside the USA, you are doing okay by USA laws as well.

Cryptography http://www.cryptography.com/index.html

A lot of background information on cryptography

Computer Security/Hackers and Culture

AT & T Research - USA http://www.research.att.com/work/
ftp://research.att.com/dist/mab/keylength.txt
ftp://research.att.com/dist/mab/key_study.txt

This site has interesting research reports which can be downloaded.

Computer Professionals for Social Responsibility (CPSR) - USA http://www.cpsr.org/dox/security/index.html

Various resources from CPSR and links to other sites

Finjan Software Ltd. - Israel http://www.finjan.com/

Security products against ActiveX and Java Internet attacks.

National Computer Security Association - USA http://www.icsa.net/vulnerabilities/

Latest security alerts for information systems, Intranets and Internet.

Computer Emergency Response Team http://www.cert.org/
ftp://ftp.cert.org/pub/

Provides latest information on software bugs with security implications. You should subscribe to the E-mail newsletter, see section further below!

Government Policy for the Internet and E-Commerce

Center for Democracy and Technology - USA http://www.cdt.org/

This non-profit organization's mission is „... to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies." Great resource for new legislative efforts in the USA as well as international lobbying efforts by business and/or advocacy groups about telecommunications and the Internet.

Encryption Policy Resource Pages - USA http://www.crypto.com/about/

This is „... an issues-oriented place on the Web for information about the United States' antiquated encryption export restrictions." Also provides one with text of proposed and enacted legislation in the USA. The site also offers free research reports on the topic.

European Commission Legal Advisory Board http://www2.echo.lu/legal/en/labhome.html

This page is provided as a service to the growing number of users around the globe interested in legal questions of the information society, particularly those related to information content, and contains updated information and relevant links regarding

the latest European and international developments, including legislation and consultative documents.“ Most documents are available in several languages.

Crypto Law Survey – The Netherlands http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm

This survey gives an overview of the current state of affairs, with entries per country on import/export controls, domestic laws, developments to restrict cryptography, and developments favoring crypto use.

Viruses and Other Issues

General anti-virus/security resource - Europe http://security.WebUrb.dk

Interesting links to many other sites around the world.

Virus hoax http://www.drsolomon.com/special/

Some background information on the most interesting virus hoaxes.

Moderated Newsletters and Listservers Worth Looking at

Computer Emergency Response Team http://www.cert.org/
ftp://ftp.cert.org/pub/
Subscribe to CERT advisories by E-Mail to cert-advisory-request@cert.org

Provides latest information on software bugs with security implications.

Computer Underground Digest - USA http://sun.soci.niu.edu/~cudigest/

This digest has interesting information about legal developments as well as sub-cultures (e.g., hackers)

Online Advertising Discussion List/Archives - USA http://www.o-a.com/

The page states that the „Online Advertising Discussion List focuses on professional discussion of online advertising strategies, results, studies, tools, and media coverage.“ As such it also addresses security and privacy issues from a marketing perspective. Instead of subscribing, why not simply check the archives from time to time and read what is of particular interest to you.

Internet Scambusters - USA http://www2.scambusters.org/scambusters/

Sheds the hype and scams from the beef, free newsletter about current Internet scams and other pertinent information

Lambda Bulletin - France
Subscribe to newsletter by E-Mail to subscribe lambda-en "Urs E. Gattiker"

Archive http://www.freenix.fr/netizen/

This newsletter deals with encyrption, privacy and security matters in France as well as other countries (e.g., Vietnam and China). An English version is available (see – en above). Definitely non-USA focus which is helpful for most of us working in this area.

Media Professional -- USA — Subscribe/Unsubscribe: MediaProfl@aol.com

The focus of this newsletter is: „Making print and online media work for you. Published the first of each month by the Young Media Professionals Committee of the Audit Bureau of Circulations.“ As such it discusses Internet marketing issues including privacy concerns related to direct marketing, advertising and tracking web site visits by end-users.

Red Rock Eater News Service (RRE) - USA — rre-help@weber.ucsd.edu

E-Mail newsletter service with a wild but interesting collection of items in the area of computer security, privacy, ethics and many more. Send an empty E-Mail for further information on the RRE.

The Risk Forum Newsgroup - USA — comp.risks
Subscribe to newsletter by E-Mail to — risks-request@csl.sri.com
Archive — ftp://ftp.sri.com/risksftp://ftp.sri.com/risks

Provides information on various risk issues in the digital world.Read the newsgroup or subscribe to the E-Mail newsletter.

TIM-SecurityNews – Europe/Asia — http://Security.WebUrb.dk

Subscribe to newsletter by E-Mail to:
TIM-Security.Subscribe@News.WebUrb.dk

The listserver will ask you to confirm that you have subscribed for security reasons. Once you have confirmed your subscribing to the newsletter by using the reply option, you are automatically registered.

Archive — http://Security.WebUrb.dk, click on News

TIM-ResearchNews is a collaborative effort between TIM-Research and EICAR's Ad-hoc Working Group Trust in E-Commerce. WG Trust in E-Commerce of EICAR focuses on information safety, security, privacy, property as well as e-commerce issues and fighting spamming. TIM-Research is a virtual research organisation focusing on matters involving new technologies and innovation.

EICAR-Conference News- EICAR Annual Conference — http://www.EICAR.dk/

Subscribe to newsletter by E-Mail to:
eicar-conference.Subscribe@News.WebUrb.dk

The listserver will ask you to confirm that you have subscribed for security reasons. Once you have confirmed your subscribing to the newsletter by using the reply option, you are automatically registered.

Archive — http://www.EICAR.dk/Newsletters

EICAR brings together technical, security and legal experts from different backgrounds. EICAR combines academic, private sector, civil, military and law enforcement expertise. EICAR represents united efforts against the writing and proliferation of malicious code, computer crime, fraud and misuse of computer networks.

REFERENCES

Abelson, H., Anderson, R., Bellovin, S.M. Beneloh, J., Blaze, M., Diffie, W. Gilmore, J., Neumann, P.G., Rivest, R.L., Schiller, J.I., Schneider, B. (1997). **The risks of key recovery, key escrow, and trusted third-party encryption**. (ftp://research.att.com/dist/mab/key_study.txt) (July 1, 1997).

Akdeniz, Y. (1998). **No chance for key recovery: Encryption and international principles of human and political rights**. Working Paper, University of Leeds, UK.

Anderson, R. (January 12, 1996). **Security in clinical information systems**. (http://www.cl.cam.ac.uk/ftp/users/rja14/policy.txt) (January 23, 1998).

Avrahami, R. (October 6, 1996). List sale case to the VA Supreme Court. **Computer Privacy Digest, 9** (23), pp. 3-4 (<comp-privacy@uwm.edu>)

Bill 68 1993, Chap. 17 (August 4, 1993). An act respecting the protection of personal information in the private sector. **Gazette Officielle du Québec, 125**, 4253-4279.

Blaze, M., Diffie, W., Rivest, R.L., Schneier, B., Shimomura, T., Thompson, E., Wiener, M. (1996). **Minimal key lengths for symmetric ciphers to provide adequate commercial security.** (ftp://research.att.com/dist/mab/keylength.txt) (July 10, 1997).

Bloom, P.N., Milne, G.R. & Adler, R. (1994). Avoiding misuse of new information technologies: Legal and societal considerations, **Journal of Marketing, 58**, 98-110.

Bundesministerium fuer Bildung, Wissenschaft, Forschung und Technologie (October 8, 1997). **Verordnung zur digitalen Signatur** (Signaturverordnung – SibV). (Regulation for digital signatures) (http://www.iid.de/rahmensigv.html) (February 28, 1998) (unofficial English translation can be found at (http://ourworldcompuserve.com/homepages/ckuner).]

Council of Ministers (August 5, 1997). **Schema di Regolamento Atti, documenti e contratti in forma elettronica** (regulatory framework for electronic documents and contracts in electronic form). Approved by the Italian Council of Ministers.

Council Regulation (EC) 3381/94, (December 19, 1994**) Setting up a community regime for the control of exports of dual-use goods**, OJ L 367/1, 31.12.94. Council Decision 94/942/CFSP, 19.12.94 establishes the lists of dual-use goods covered by the Regulation, OJ L 367/8, 31.12.94.

Coughing up. (1997, October 25). **The Economist**, p. 94.

Cryptographic algorithms (not dated). (http://www.cs.hut.fi/ssh/crypto/algorithms.html) (Accessed July 15, 1997).

Culnan, M. J. (1993). „How did they get my name?“: An exploratory investigation of consumer attitudes toward secondary information use. **MIS Quarterly, 17**, 341-363.

Directive of the European Parliament and the Council (adopted by the Council on 24th of July, 1995). On the protection of individuals with regard to the processing of personal data and on the free movement of such data (final). Bruxelles: The Author.

Denning, D. E., & Baugh, W. E. Jr. (1997). **Encryption and Evolving Technologies as Tools of Organized Crime and Terrorism.** (http://guru.cosc.georgetown.edu/~denning/crypto/oc-abs.html) (December 15, 1997).

Donaldson, T. & Preston, L. (1995) The Stakeholder Theory of the Corporation: Concepts, Evidence and Implications. **Academy of Management Review, 20** (1), pp. 65-91.

Doss, E. & Loui, M.C. (1995). Ethics and the privacy of electronic mail. **The Information Society, 11**, 223-235.

DTI (1997). Licensing of TTPs for the provision of encryption services - **DTI Public Consultation Paper # 3***.* Brussels: The Author (http://www.dti.gov.uk/pubs/) (December 17, 1997).

European Commission, **Telecommunications, Information Market and Exploitation of Research** (October 1997). Ensuring security and trust in electronic communication. Brussels: The Author (COM(97)503

Freeman, R. E. (1984) **Strategic Management: A Stakeholder Approach**. Boston, MA: Pitman.

Gattiker, U. E. & members of EICAR Working Group 1. (**1997**). Internet security: Strategic and social issues. **Proceedings of the European Institute for Computer Anti-Virus Research (EICAR) 1997 Security Workshop, Hamburg, Germany** (pp. 173-211) (see also http://tim.weburb.dk/index.php3?src=13

Gattiker, U. E., & Kelley, L. (1999). Morality and computers: Attitudes and differences in moral judgments across populations. Information Systems Research, 10, 223-254.

Gattiker, U. E., Kelb, J., Janz, L., Holsten, H., Greshake, J., Schwenteck, O., & Miller, J.(1997). Direct marketing and privacy for telephone and internet users: A South African field study. **Global Business in Practice. Proceedings of the Tenth International Bled Electronic Commerce Conference, Bled, Slovenia,** 604-639.

Giussani, B. (1998, 24. February**).** An Appraisal or technologies of political control. **Eurobites**, p. 1.

Gostin, L. O., Lazzarini, Z., Flaherty, K. M. (not dated) **Legislative survey of state confidentiality laws, with specific emphasis on HIV and immunization**. (http://epic.org/privacy/medial/cdc_survey.htm) (July 18, 1997).

Government introduces draft legislation to protect the privacy of health information (June 11, 1997). (http://www.gov.ab.ca/~pab/4984.html) (October 28, 1997).

Harely, D. (1998). Re-floating the Titanic: Dealing with social engineering attacks. **Proceedings of the European Institute for Computer Anti-Virus Research (EICAR) 1998 Conference on „Web-Safety“ Munich, Germany** (pp. 1-27).

Information Policy Committee, National Information Infrastructure Task Force (April, 1997). **Options for promoting privacy on the national information infrastructure**. (http://www.iitf.nist.gov/ipc/ipc-pub.html) (July 22, 1997).

Katsh, E. (1994). Privacy and new information technologies. Paper delivered **to 18th Regional Conference the History and Philosophy of Science, University of Colorado, Boulder, Co.**

Loi N° 90-1170 (29 December 1997). Article N° 28. Telecommunications law. (http://www.legifrance.fr) (Accessed March 1, 1998). This law is currently being modified according to loi N°96-659, 26.7.96 de réglementation des télécommunications art 17; (http://www.telecom.gouv.fr/francais/activ/telecom/nloi17.htm) (December 17, 1997)

March, J. G., & Simon, H. A. (1958). **Organizations**. New York: John Wiley.

McClosky, H. & Brill, A. (1983). **Dimensions of tolerance: What Americans believe about civil liberties.** New York: Russel Sage Foundation.

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. **Academy of Management Review, 22**, 853-886.

NCSA (National Computer Security Association) (July 1997). Firewall user profile. **An NCSA focus report. Carlisle, PA**: The Author.

OECD (1997). **Report on background and issues of cryptography policy**. Paris: The Author.

OECD (November 1980**). OECD Guidelines governing the protection of privacy and transborder flows of personal data**. Paris: Author.

Pitchford, R. A., & Kay, S. (1995). GP practice computer security survey. **Journal of Informatics and Primary Care**, September, 6-12.

Privacy International. (1996). The Universal Declaration of Human Rights. URL:http://www.privacy.org/pi/intl_orgs/un/intl-decl-human-rights.txt (February 11, 1998).

Schlossberg (1993). Victims tired of researchers getting away with murder. **Marketing News**, August 16, A16, 1.

Sequoia Software chosen to link U.S. patient records (October 24, 1997) (http://www.microsoft.com/industry/health/press/Sequoiapr.htm) (January 23, 1997).

Spriggs, M. T., & Nevin, J. R. (1996). Negative option selling plans: Current forms versus existing regulations. **Journal of Public Policy & Marketing**, 15, 227-237.

Strategic partner selected to develop a blueprint for an Alberta health information system (July 14, 1997). (http://www.gov.ab.ca/~pab/5130.html) (October, 28, 1997).

Striking the right balance. Access to health information (December 5, 1996). (http://www.health.gov.ab/access.htm) (July 21, 1997).

Swiss police have secretly tracked the whereabouts of mobile phone users via a telephone company computer that records billions of movements going back more than half a year (as reported in a Swiss Sunday newspaper), (Dec 28, 1997). Reuters.

Szlovits, P., Doyle, J., Long, W. J., Kohane, I., & Pauker, S. G. (May 1994). **Guardian angel: Patient-centered health information systems.** (http://medg.lcs.mit.edu/project/ga/publications.html) (July 19, 1997).

Towards a European framework for digital signatures and encryption (October 8, 1997**). European Internet Forum Policy Papers** (http://www.ispo.cec.be/eif/policy) (October 13, 1997).

The people vs. AOL (Winter 1998). Adbusters. **Journal of the Mental Environment, No. 20**, p. 60.

The Wassenaar arrangement on export controls for conventional arms and dual-use goods and technologies (December 20, 1995). (http://ideath.parrhesia.com/wassenaar/wassenaar.html) (March 4, 1998).

Thorel, J. (18 December, 1997). Frenchy Cryptosoap #123578. **Lambda**, 3.08, p. 1 (see also http://www.freenix.fr/netizen/chiffre/avis-cssp.html).

Ulhøi, J. P. (1997) A stakeholder approach to green innovation. **In Proceedings of The Fourth International Meeting of the Decision Science Institute, Sydney**, 34-77.

Ulhøi, J. P. & Madsen, H. (1998) Greening of industry in a push-pull stakeholder perspective. Theory, experiences and implications. Working Paper, Aarhus School of Business.

van Swaay, M. (1995). The Value and Protection of Privacy. **Computer Networks and ISDN Systems, 26** (Suppl. 4), 149-155.

Walsh, G. (October 1996). **The Walsh report**. (http://www.efa.org.au/Issues/Crypto/Walsh/Walsh.htm) (August 31, 1997).

Table 1

Security of Information Systems

Security Issue	Description	Application to Medical Information and Data
1. Confidentiality of Data	Is the property that data or information is not made available or disclosed to unauthorized, parties (e.g., individuals, organizations and processes)	Medical data is not being disclosed to others, such as employers. making the identification of the patient possible.
2. Integrity of Data	Is the property that data and information has not been modified or altered in an unauthorized manner?	Unauthorized personnel are unable to alter medical records while changes made by others are tracked and recorded.
3 Availability of Data	Is the property that data and information, as well as the necessary systems, are all accessible and useable on a timely basis as required to perform various tasks	Medical personnel must get access to patient files even during a massive power outage where generators may have to be used to guarantee availability of data

Note. To improve confidentiality, integrity and availability of data, encryption may have to be used, thereby reducing the information's vulnerability to attacks against its confidentiality and integrity. Naturally, encryption can also help in reducing risks of such attacks in succeeding and compromising medical information (e.g., misuse or alterations). Conceptual and practical suggestions about reducing information systems vulnerabilities and risks can be found in Gattiker and members of EICAR Working Group 1 (1997) (see Tables 3 & 4, Figures 1 & 2).

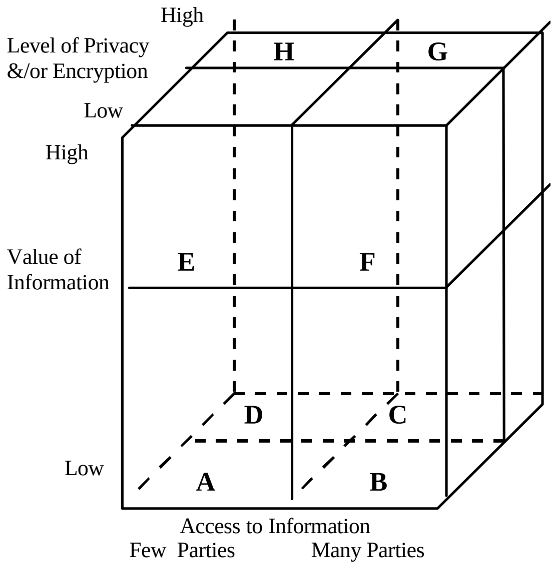

Figure 1. A model for classifying challenges against encryption of medical data and its privacy and safety/security

Table 2

Factors Influencing the Likelihood of Information Being Disclosed to Various Stakeholders

---

1) ***its value*** (e.g., to the insurer, employer and patient) (see also Section 2.3.)

2) ***the number of stakeholders and people who have access to the information****, and*

3) ***legitimate versus illegitimate access to information*** by stakeholders and others.

Note. The above factors increase the threat against maintaining database confidentiality, integrity and availability at all times (see Table 1). Managing these factors may also be facilitated by determining the financial value of the medical data (e.g., if lost or altered). Accordingly, liability costs for violations against trust and generally accepted safety and security standards resulting in damaged data and/or illegitimate access to information can be determined (see also Section 2.3.).

Table 3

Factors Facilitating Efforts for Maintaining Confidentiality, Integrity and Availability of Medical Data

The challenge is to strive for:

1) complete and accurate information in the medical database, which is of substantial value to various stakeholder groups, while in turn

2) limiting the number of people getting access and, most importantly,

3) assuring privacy by using encryption and other methods to prevent unauthorized parties from getting access to medical data files kept in an information system.

Note. The above factors are in apparent conflict because the greater the completeness and accuracy of the database, the more groups and individuals want access (Point 2), and thus the greater the difficulty to maintain privacy.

Table 4

Calculating Hard and Soft Costs of Security and Safety „Disasters“: Asset Value

---

Of interest here is what it would cost to get a damaged/compromised medical database running again and/or re-create information, databases, files (e.g., password), etc.:

$$\sum \text{ Costs} = \sum \text{HC} + \sum \text{SC} \quad (1)$$

Where **HC** are the **hard costs** (e.g., human resource costs for working hours lost and overtime needed to cope with the backlog of unprocessed work amassing rapidly on one's desk) and **SC** are the **soft costs** (e.g., opportunity costs due to downtime of machine/system). Additionally, we can expand the above formula as follows:

$$\sum \text{ Costs} = \sum \text{HC (FC +VC)} + \sum \text{SC (FC + VC)} \quad (2)$$

FC are **fixed costs** (e.g., fixed charge by computer service to do a „house call“, based on Shadow Pricing) and **VC** are **variable costs** (e.g., hours not working due to personal computer being down or hard disk crashed)

Hard Costs may also entail costs for new hardware and software required to fix the problem.

Incurred costs by a patient are usually **HC** and **VC**, i.e., sometimes we can calculate them and they are variable. For instance, if a hacker alters a patient's record, correcting the record on the database costs (e.g., system expert's time) but, most importantly, the patient's life may be at stake if given the wrong blood or drugs during emergency treatment. Hence, the difficulty will be to determine the likelihood of such outcomes (death due to wrong treatment, latter was caused by party gaining illegitimate access to data and altering it incorrectly) as well as the value of damages caused to the patient by such outomes.

Shadow pricing is a concept used by economists to determine the price for a product and/or service for which the firm may not have a clear idea or formula for calculating realistic costs. Here economists suggest we look at the market price for the product/service we need. In the case of wrong information or illegitimate access to the medical database, the patient and/or the patients physician may both claim damages against the party managing the database on behalf of the government. Here previous product liability and/or malpractice lawsuits may help in determining the costs. In turn, these figures from previous lawsuits in conjunction with the likelihood of such outcomes represent a shadow price for the **fixed costs** (FC) incurred by the firm to fix a medical problem/disaster (e.g., death of patient due to wrong blood type used for transfusion).

Soft costs (SC) (see Equations 1 and 2) are more difficult to calculate than the hard costs (HC) since we have to determine the value of information which in itself is a subjective process. For instance,

1) what is the value to the firm (i.e. medical database administrator or health agency) of a password file with 1200 accounts?

2) How much does it cost the firm or medical community including patients if the database is down for eight hours during the night and medical personnel are unable to access it to provide emergency health care?

3) What are the costs for lost data/files due to a failure of a hard-disk for a notebook computer in a doctor's office assuming that the last back-up was done 12 hours ago?

4) What are the costs of lost material (e.g., sentences typed using a word processing program between the last automatic update and the system crash) because of random system crashes (e.g., with an old version of Windows 95) whereby software is being closed by the operating system (e.g., this could happen to 50% of end-users at least once a day) due to flaws in the latter?

5) How dependable is the firm on the IS, asset, property and more which could be damaged because of a threat or a vulnerability; can medical personnel perform important work when the system is down?

$$\sum \text{ Soft Costs (SC)} = \sum \text{FC (CF +R\&D/C)} + \sum \text{VC (OC + NR\&D/C + AC)} \quad (3)$$

In Equation 3, **CF** are the **confidence costs** incurred by the „disaster“, i.e., every time a system is being shut

down or data is being lost, users (including doctors and patients) lose confidence and require additional measures to feel safe (e.g., faxing a medical datafile in addition to accessing information on-line). In turn, the company has to put effort into reassuring users of the reliability of the system which takes resources (human and others). **R&D/C** are the **research and development costs/expenditures** which may be lost due to having confidential information about a patient being released to the wrong party.

If we look at the **VC** part of Equation 4, **OC** represents the **opportunity costs** incurred due to the disaster (e.g., crashed system disk) where medical personnel could perform surgery needed by a patient instead of trying to keep a patient stable until receiving data from the patient's medical file.

NR&D/C are the **new research and development costs** which must be absorbed by the firm in order to either re-establish the medical database.

AC are the **additional costs** a firm may incur such as training/support of employees for retooling recovered system/data files, as well as the costs of lost productivity (e.g., health professionals are unable to perform their tasks because of system down-time, also dependability on the system).

$\sum$ Asset Value of the Object(AVO) = Equation 1 + AVO (SP + CAI) (4)

Besides the costs as calculated with Equation 4 (see Equations 2-3 for details), **AVO** represents the **asset value of the object** (e.g., data file, software, Web page system and much more). Again, **shadow pricing** (**SP**) plays an important role here whenever internal costing is difficult (e.g., internal pricing may not reflect market prices). Also components internally developed may be assigned a value using **cost accounting** (**CA**) to determine the **investmen**t (**I**) required to design and implement various components of the system.

Note. The above presents a possible approach for assessing the asset value of the object (**AVO**) for information resources. Part of the above Table is derived from Gattiker and Wg1 (1997), while some additions have been made to make the approach applicable to medical databases.