Study on Legal and Regulatory aspects of eHealth "Legally eHealth" : deliverable 5 : final recommendations on legal issues in eHealth

Herveg, Jean

Publication date:
2006

Document Version
Publisher's PDF, also known as Version of record

European Commission
Contract # 30-CE-0041734/00-55

Study on Legal and Regulatory Aspects of eHealth

"*Legally* eHealth"

DELIVERABLE 5

FINAL RECOMMENDATIONS ON LEGAL ISSUES IN EHEALTH

Start Date:	1st January 2006
Commencement date of Contract:	1st January 2006
Duration:	12+3 months
Contractor:	European Health Management Association
Version:	10 final

Deleted: 9

TABLE OF CONTENTS

INTRODUCTION TO THE STUDY

The concept of eHealth and its reality in daily medical practice fundamentally challenges our understanding of the practice and regulation of healthcare in terms of the relationship between practitioner and patient, between practitioner and institution as well as between institutions.

In the traditional model, patient access to the healthcare delivery system has been limited to predetermined points of entry, such as through a primary care physician. From the entry point, the patient's progress through the system has been relatively linear and often dictated by the health system's reimbursement systems. Similarly, processes such as diagnosis, treatment and care have involved physical presence and personal interaction between providers and patients and of course, such physical presence requires some sort of identification (i.e., lack of anonymity).

eHealth, however, is premised on a fundamentally new patient experience that is unconstrained by familiar points of entry and structures or traditional channels for delivering information or care. For one thing, anonymity or pseudonymity can be preserved much more easily. Not surprisingly, therefore, the eHealth revolution has as many serious implications for healthcare regulators and lawyers as for medical professionals.

Although policy makers have noted at both European and national level that a lack of legal certainty about the use of eHealth tools and services exists, little has been done to study the issue in detail. Certain projects[1] funded under the Framework Programmes have looked at the general legal issue concerning the use of information society technologies (IST), while others have included work packages looking at the legal aspects of a particular technology or application[2]. Others still have looked at one particular issue, such as confidentiality, in greater detail[3]. However, it would seem that no work has been undertaken to date to look across the whole range of legal issue relevant to the use of IST tools and services in healthcare and to draw conclusions about the regulatory needs which may exist.

As long ago as 1999, when the European Commission launched the *e*Europe initiative with the adoption of the Communication '*e*Europe – An Information Society for All' (COM(1999)687 final, of 8.12.1999), it was noted that although the market for technological applications in the clinical domain was developing rapidly in Europe, and although the increase of health related information and education material available on the internet was of growing significance, the full exploitation of both sectors of eHealth was hindered by a *lack of legal clarity and certainty*. The Communication noted specifically that, in the clinical (including commercial) eHealth applications domain "uncertainty persists in the health telematics related industry about responsibility and data protection, the legality of providing on-line medical opinions as well as on-line pharmaceutical information and product supply."

1 see for example Legal IST- FP6-IST

2 see for examples NEXTGRID - FP6-IST or EUROGENTEST - FP6-LIFESCIHEALTH and FP5-GEMSS

3 see for example EUROSOCAP – Quality of Life Programme (FP5)

Deleted: FP6

The issue was raised again in the 2004 Action Plan for a European eHealth Area (COM(2004)356). This stated that despite adoption of EU legislation on issues such as Data Protection (95/46/EC), Electronic Signatures (99/93/EC), eCommerce (2000/31/EC), Distance Contracting (97/7/EC) and the existing legislation on General Product Liability (92/59/EEC) and on Medical Devices (93/42/EEC), considerable uncertainty on the legal aspects of the use of eHealth applications, tools and services still continues. Accordingly the Action Plan proposes that by 2009 the European Commission shall "provide a framework for greater legal certainty of e-Health products and services liability within the context of existing product liability legislation."

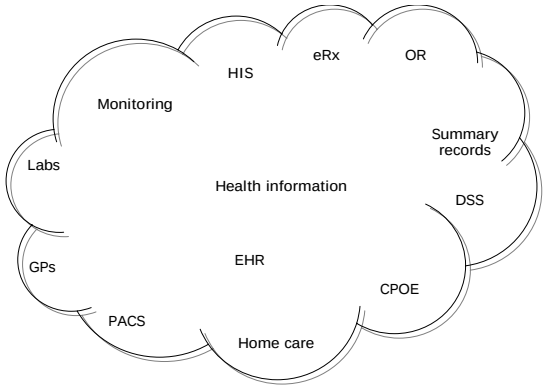
In this context, the Commission called for the present study in order to establish a baseline report on existing EU level legislation, its impact on the delivery of eHealth and an analysis of the legal lacunae that may exist. The "Legally eHealth" study has looked in detail at three key regulatory aspects and has analysed the ways in which they might apply to eHealth situations: privacy, liability and competition.

In this final report we look at which gaps might be said to exist - in how far is the regulatory framework that currently exists at European level sufficient to allow this important sector of European industry to flourish? We ask if in fact there are still significant barriers to the adoption and full exploitation of eHealth tools, systems and services to be found in a lack of relevant regulation.

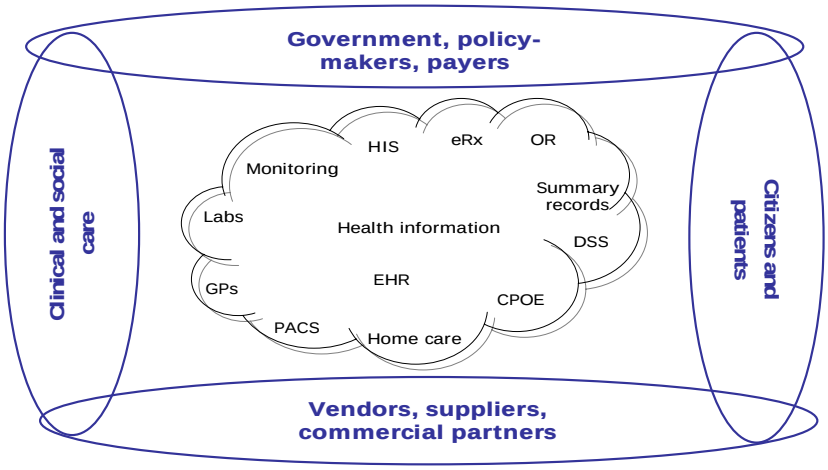
In keeping with the structure of the study this report looks first at the general legal issues in eHealth, then in some detail at the three areas discussed in the three core deliverables and finally at any other outstanding legal questions.

SETTING THE SCENE ON OUR EHEALTH WORLD

eHealth is a very broad term and encompasses many concepts. In this study we have taken the term to include the wide range of information technology based applications found in hospitals and primary care settings. These include administrative tools such as hospital information systems (HIS), summary records and discharge letters, clinical technical applications such as picture archiving and communications systems (PACS) as well as clinical support systems such as operating theatre systems (OR), decision support systems (DSS) and systems linking intuitions such as General Practitioners Systems, and electronic prescribing systems linking general practitioners with pharmacies (eRx). At the heart of our eHealth world is the elusive holy grail of eHealth – the fully interoperable cradle to grave Electronic Health Record.



The stakeholders in eHealth World are classified into four groups of actors: citizens and patients; clinicians and care providers; payers, policy-makers and governments; and vendors, suppliers and commercial partners. All four groups of actors have highly significant but not always equal roles to play in healthcare. Our study in particular looks at the tensions that can arise between clinician and patient with respect to privacy and confidentiality or between government and vendor with respect to competition in the healthcare market.



The Policy Context

Before looking in some detail at the extent to which European law regulates eHealth it is important to step back and consider the role of Europe in health. For the European Union, which in 2007 celebrates its 50th Anniversary, public health policy is a relative new-comer arriving only in 1992 when the Maastricht Treaty included an article on "encouraging cooperation between Member States" and "if necessary, lending support to their actions" in public health. This legal competence was strengthened in 1997 with the Amsterdam Treaty when the EU was mandated to ensure "a high level of human health protection" in the "definition and implementation of all [Union] policies and activities" and to work with Member States to improve public health, prevent illness and "obviate sources of danger to human health" (article 152(1)).

While the Amsterdam amendment extended the scope of public health related policy, it maintained the 'subsidiarity principle' for health which provides that harmonisation of Member Sates' public health legislation is prohibited and the Union shall continue to respect fully the Member States' responsibilities for the organisation and delivery of health services and medical care (article 152(4, 5)).

The current situation is therefore that the European Union has a limited mandate to adopt public health policy whilst at all times respecting the right of Member States to adopt national level measures to regulate the organisation and delivery of health services. Thus even where EU level legislation on blood, organs and tissues is provided for in article 152(4)(a), the Treaty highlights that such legislation shall not prevent any Member State from maintaining or introducing more stringent protective measures.

Given that direct health policy is limited by the principle of subsidiarity it might be thought that there is rather little health services related law at EU level. As already outlined, this study considers data protection law, consumer protection law and competition law, but it should not be thought that these three areas of law denote the limits of EU law and health.

It is worth noting, for example, that European employment law has had a considerable impact on the organisation of health services in the EU in recent years. The Directive on the Organisation of Working Time, for example, which established the general principle that no employee can be obliged to work more than 48 hours a week and laid down minimum daily rest periods, has led many countries to adopt new contracts and procedures to govern the work of medical staff. Similarly the Directive on the Recognition of Professional Qualifications has simplified the mobility of health professionals across internal borders and has led some Member States to re-assess their medical education programmes.

It is not, however, only employment related issues which impact on health; many other policy areas have had a significant impact on health and health services. The current debate at EU level on the approximation of the laws of the Member States relating to the labelling, presentation and advertising of foodstuffs requires all ingredients to be indicated on the label of food products and obliges manufacturers to list 12 potentially allergenic ingredients, in order to help consumers with health conditions or food allergies avoid specific ingredients or substances.

However, the most well known legal aspect of health services in the European Union is related to the four fundamental freedoms of European citizens: the freedom of movement of goods, capital, services and persons. The free movements of goods and capital have almost been achieved, not least through the adoption of the single European currency. The full integration of the free movements of services and people has, however, been slower to achieve since they both have significant ramifications well beyond the economic sphere.

The freedom of personal movement was initially construed as an objective applying only to workers, but as the European Union integration has deepened so a wider interpretation has come to prevail, not least through Directives which provide rights of residency for students and retired people and allow free movement of EU citizens provided they can show adequate financial means to support themselves. Through these provisions, it has become accepted that so long as an EU citizen has an independent income or a job he or she is entitled to settle in any EU Member State. Furthermore the European Court of Justice has stated that restrictions may only be imposed in individual cases where there is sufficient justification.

The free movement of services is closely linked to the free movement of persons since it provides for professionals to practise anywhere in the EU in order to offer their services. The current rules lay down that, save for certain exceptions based on public policy, a provider of services is entitled to offer his or her services in an EU Member State other than his or her own, or to offer such services to someone who travels from another Member States in order to avail of services outside their normal country of residence.

The development of the free movement of goods, services and people with respect to health related issues is found in the interpretation of the European Court of Justice of the rights accorded to European citizens under Regulation 1408/71 on the application of social security schemes to employed persons and their families moving within the Community.

Since 1998 a series of highly significant cases have clarified the rights of European citizen to make use of health services and goods provided in Member States other than their usual State of residence. Of particular relevance are the Kohll case[4], which provided that dental services are subject to the rules of free movement of services in articles 49 and 50 TEC, and the Decker case[5] in which the Court held that prescription spectacles were covered by the provisions on the free movement of goods in articles 31 and 39 TEC. The later cases of Geraets-Smits/Peerbooms [6] and Mueller-Fauré/van Riet [7] addressed the issues of free movement to obtain hospital treatment out of state.

The development began in 1998 when two Luxembourgish men purchased orthodontic treatment (Kohll) and spectacles (Decker) outside Luxembourg. In both cases the parties had purchased health services or goods in another EU Member State without obtaining the prior permission from their health insurance schemes provided as for in Regulation 1408/71

4 Case C-158/1996 of 28 April 1998
5 Case C-120/1995 of 28 April 1998
6 Case C-57/99
7 Case C-385/99

and then sought reimbursement of their expenses from their local Caisse de Maladie at normal Luxembourgish rates.

Mr Kohll argued that the prior authorisation system restricted him from purchasing services in contravention of article 59 and 60 of the Treaty while Mr Decker maintained that his right to buy goods protected under article 30 was similarly violated.

The European Court of Justice heard the cases jointly and determined that access to health services and the provisions of the Treaty covered health goods. The Court stated that while Regulation 1408/71 was valid, it as nonetheless secondary law, placing health services within the reach of the Treaty. Consequently, the Court held that the Treaty provisions on free movement of goods and services apply to health goods and services, thus providing a means for obtaining health goods and services in another state.

Having established that principle, the Court next had to decide if the rules in 1408/71 that require the citizen to obtain prior authorisation before accessing such goods or services was a justifiable impediment to the general rule on the basis of public health or public policy. In each case, Luxembourg argued that the requirement of prior authorisation was a justifiable restriction on the basis that it was necessary to ensure the financial balance of the social security system and to safeguard to quality services and goods delivered.

The Court dismissed the first argument on the basis that, since the reimbursement sought was at Luxembourgish rates, the local insurer would not have to pay out more than if the services or goods had been obtained in Luxembourg. The Court did accept, however, that in principle the need to ensure a balanced medical and hospital service open to all might justify limits on cross-border access to certain types of health services. Luxemburg's second argument, that free access to health goods and services across internal borders should be limited on the basis of ensuring high quality, was dismissed on the grounds that the mutual recognition qualifications legislation provided adequate surety of the quality of health services providers in other EU countries.

The following cases all tested the extent of the Court's acceptance of the concept that prior authorisation for hospital-based health services could be justified and that therefore if a citizen failed to obtain such authorisation he or she could not seek reimbursement for any treatments obtained.

The Geraets-Smits/Peerbooms case involved two Dutch claimants. Mrs Geraets-Smits had Parkinson's disease and was treated in a specialist clinic in Germany. Her sickness insurance fund refused reimbursement of the costs incurred, on the ground that satisfactory and adequate treatment for that disease was available in the Netherlands and that the treatment provided in Germany conferred no additional advantage. Mr Peerbooms fell into a coma following a road accident. He received special intensive therapy in an Austrian clinic because he did not satisfy the requirements for the treatment in the Netherlands where it was available only to persons under the age of 25 years. Neither patient had obtained the prior consent for treatment outside the Netherlands provided for in the national legislation.

In both cases the Court observed again that Member States are free to organise their social security systems, and recognised that a prior authorisation scheme could fit this need. In

each case the Court decided however that the grounds given for refusing the prior authorisation were not justifiable and did not satisfy the principle of proportionality. The Court held that authorisation may be refused only if the patient can receive the same or equally effective treatment without undue delay from an establishment with which his or her sickness insurance fund has contractual arrangements.

In the Mueller-Fauré/van Riet case, the Court further clarified that in determining undue delay for access to hospital care national authorities must take account of the patient's actual medical condition and, where appropriate, the degree of pain or the nature of the patient's disability, which might, for example, make it impossible or extremely difficult for him or her to carry out a professional activity, but also of his or her medical history. For the case of non-hospital care, the Court held that the principle of freedom to provide services precludes legislation that requires the insured to obtain prior authorisation for non-hospital care provided in another Member State by a non-contracted provider.

On the matter of the level of costs to be reimbursed, the Vanbraekel[8] case provided that national legislation must guarantee that an insured person who has been authorised to receive hospital treatment abroad receives a level of payment comparable to that which he or she would have received if he or she had received hospital treatment in his or her own Member State, even if in some cases this might result in a patient obtaining reimbursement at the national rate which is higher than the actual costs incurred in another EU Member State.

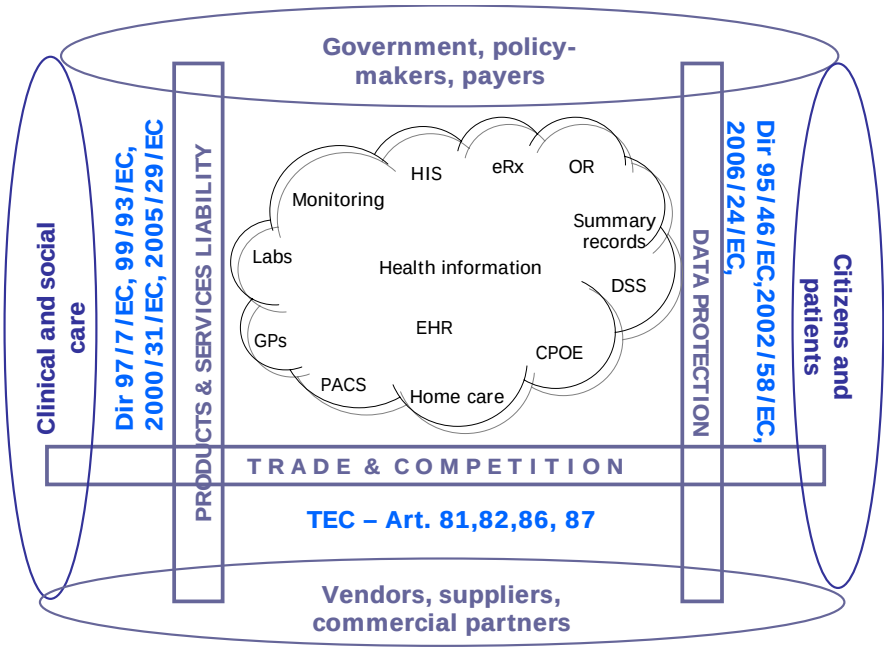
It may be seen therefore from this array of cases that the European Court has decided quite firmly that:

- Health services are services within the meaning of the Treaty and that therefore the rules on freedom of movement to obtain such services apply to European citizens seeking health services outside their own Member State;
- Member States have a justifiable interest in limiting free access to health services in other Member States if to do so is necessary for planning and financial balance of health services;
- Systems of prior authorisation may be used to facilitate planning of hospital based services, but not for non-hospital care;
- Prior authorisation must be granted if equivalent treatment cannot be offered in a reasonable time having regard to the specific characteristics of the patient.

8 Case C-368/98

LEGALLY EHEALTH – SETTING THE LIMITS

The study notes the issues around freedom of movement as discussed above but concentrates in particular on three areas of European law rarely considered in depth with respect to health policy, and more rarely still with respect to eHealth.



The "Legally eHealth" study in its three core chapters therefore considered the impact of data protection legislation, consumer protection and liability legislation and competition law.

Deliverable 2 looks in detail at the requirements of EU and international level privacy and data protection legislation. It provides a thorough examination of the Data Protection Directive, Privacy in Electronic Communications as well as the European Convention of Human Rights and a number of recommendations of the Council of Europe. This legislation is then explored against the backdrop of a number of scenarios exploring data transfer for the purposes of better care provision both across European and international borders, as well as for commercial purposes.

Deliverable 3 looks at the vexed issue of liability of eHealth goods and services. Whilst some of the services are rather simple eCommerce services transacted over websites, much more complex issues in terms multiple and split liability for services provided through a series of co-operating providers is also explored.

Deliverable 4 considers the issues of trade and competition law that might apply to eHealth. Health services, in most European countries are provided to at least to some extent through direct taxation and compulsory health insurance. However, most eHealth services are offered through private enterprises and businesses and thus eHealth poses difficult questions concerning competition with public and private markets in situations where the distinction between the two is often very hard to establish.

Having set out the core elements of those areas of law we now consider where the gaps might lie and how the European Commission should continue to develop policy and legislative initiatives which build on the existing framework to encourage the uptake of eHealth services across the European Union.

RECOMMENDATIONS

Recommendations on Data Protection

Data Protection legislation is now well established in Europe, having its base in the Directive of 1995 which we discussed extensively in Deliverable 2. In respect to eHealth, the first point to note is that the current Directive takes a restrictive approach to health data processing – article 8 prohibits *prima facie* the processing of health data, but provides exceptions to the prohibition through patient consent, processing of data in the vital interests of the patient, processing for the purposes of medical diagnosis and care provision and in certain cases if there is a substantial public interest in such data processing.

It should be noted that the Directive does not address any particular issues related to eHealth systems and services. However, the European Working Party on Data Protection, established under article 29 of the Directive and composed of the national data protection authority of each Member State, has recently acknowledged that some special rules may need to be adopted for key eHealth applications.

To this end the Working Party issued in February 2007 a working paper looking at the applicability of data protection legislation to Electronic Health Record (EHR) systems. In its report, the Working Party noted in particular the limitation of the use of consent to permit the processing of heath data. The Working Party notes that if processing health data in an EHR system is the primary way of processing health data in a given health system, then a patient's care may be compromised if he or she opts-out of such a system by not giving his or her consent to the creation of an EHR. Accordingly, consent should not be used, as it cannot be said to be truly and freely given.

The remaining provisions setting aside the general prohibition on article 8 of the Directive can also be said to pose some problems – notably the idea that a patient ought to know the full finality of the use of data before his or her data may reasonably be used. eHealth tools such as EHRs, but also other tools used for healthcare functions such as care planning, decision support and risk assessment, are based on using the fullest range of data available to make the best informed choices.

ISSUE 1: LEGAL UNCERTAINTIES IN DATA PROTECTION AND CONSENT

Data subject consent may legitimate the processing of any data. Such consent is defined as any unambiguous, freely given, specific and informed indication of the data subject's wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed (art. 2.h). Medical data processing requires in addition that such consent be explicit because medical data is considered particularly sensitive. It is also permissible to process medical data without consent if it is in the vital interests of the data subject or another party and the data subject is physically or legally incapable of giving consent, or if it is done in the context of medical care provided by a healthcare professional with a legal obligation of professional confidentiality.

RECOMMENDATION 1: DATA SUBJECT CONSENT

As noted by the Data Protection Working Party there are some problems in using consent as a valid basis for processing data in eHealth applications. If eHealth applications are

themselves integral to the way in which a good health service is provided, then requiring consent may in fact be denying the data subject a reasonable opportunity to withhold consent. If the creation of, for example, electronic medical records is a necessary and unavoidable consequence of the medical situation, withholding consent may be to the patient's detriment. Therefore it would seem appropriate for the European Commission to co-ordinate the adoption of specific rules for the processing of health information to allow for proper balancing of patients' and public health interests, without recourse to the concept of consent.

ISSUE 2: LEGAL UNCERTAINTIES IN DATA PROTECTION AND SPECIFIED PURPOSE

Data must be collected for specified and explicit purposes. This principle requires that, prior to possessing personal data, the controller has to define clearly and precisely the purpose(s) for which the data are to be processed. Moreover, the processing should be transparent.

The data may be used only for the initial purpose and should not be re-used in a way incompatible with the initial purpose. Generally speaking, the purpose of the new processing has to be compared to the initial one(s) in order to assess whether there is a close relationship between them. A new purpose that is clearly different from the initial one(s) will be considered incompatible.

It should be noted that, if further processing is deemed incompatible with the original purpose, further processing for historical, statistical or scientific purposes may be allowed if the data subject consents or if national legislation provides for such processing.

RECOMMENDATION 2: SPECIFIED AND EXPLICIT PURPOSES

In order to make optimal use of eHealth tools the European Commission should support the adoption of guidelines on the definition of the concept of finality of purpose that would provide an adequate balance between protection of the interests of the individual on the one hand and public health management and disease prevention on the other.

If eHealth applications used for risk detection, disease monitoring and preventative care are to be fully realised, legal guidelines should be established that clarify the circumstances in which healthcare professionals can make further use of healthcare data in the interests of public health. Such guidelines should allow for secondary uses even where such uses could not have been foreseen at the time of data collection.

While most Member States have already adopted guidelines at national level for such re-use of data for research or statistical purposes efforts should be made to harmonise these approaches across the EU so that meaningful cross-border work can support the health of all EU citizens.

ISSUE 3: TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Amongst the data controller's duties are that he or she has the responsibility to protect the personal data he or she holds and therefore to take technical and organisational measures ensuring their security and confidentiality.

RECOMMENDATION 3: TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Efforts should be made to harmonise national standards on the technical and organisational measures of data security. Whilst the Data Protection Directive calls for such standards to be adopted, little has been done at a regulatory level to harmonise guidelines across the EU.

While some technical standards for security have been adopted by the CEN (Comité Européen de Normalisation), concern still exists that these standards are not sufficiently integrated into daily medical practice to ensure that healthcare professionals feel secure enough to share data across EU borders in order to provide better care for their patients.

Recommendations on eHealth and Product Liability

Traditionally, medical liability is restricted to the relationship between the patient and the health practitioner (usually a doctor). When a patient is victim of medical negligence or of a medical error the patient will usually seek to introduce a civil or criminal lawsuit against the doctor.

If medical liability continues to be considered as arising from the relationship between the patient and the health practitioner, the multiplication of intermediaries in the field of health services and the number of these with whom the patient has direct contact is changing the legal relationships between the various actors.

Although general legal rules have been agreed to provide consumers with a legal guarantee of high quality products and services, the legal texts do not specifically address eHealth. The current EU level law is applied within the general context of service provision and product delivery, whether by traditional or electronic means.

As a result it is often difficult to ascertain which EU level legislation applies to an eHealth product: is it considered a medical device, a software package, and does other legislation (e.g., on hazardous substances, for instance) also apply?

ISSUE 1: SALE OF EHEALTH GOODS

Sale of health goods, whether eHealth or traditional, will be covered by standard contracts for sale of goods. Thus, if the eHealth product fails to arrive or arrives late, the standard clauses in the contract will apply which will allow the purchaser to pay less or to return the goods. Similarly national legislation based on the EC Product Liability Directives will ensure that the purchaser has redress if the goods are not fit for the purpose for which they were sold.

In general therefore in the eHealth arena, the purchaser of an eHealth good will need to make reference to the relevant national legislation based on Directive 1999/44 on the sale of consumer goods and associated guarantee. According to this Directive, when consumer goods are sold under a contract, the seller must deliver goods in conformity of the contract of sale. Moreover, when a commercial guarantee exists, the seller or producer who offered it will be legally bound to it. Anyone selling an eHealth product would have to comply with these rules, and conversely a purchaser of an eHealth product would have redress under them.

RECOMMENDATION 1: SALE OF EHEALTH GOODS.

It is not considered necessary to adopt specific eHealth sales of goods legislation. However it might be appropriate to consider the adoption of specific EU level guidelines on the sale of eHealth goods in order to encourage the adoption of EU wide markets in eHealth tools rather than the fragmented national level markets one sees currently.

ISSUE 2: PRODUCT SAFETY

Directive 2001/95 on general product safety imposes a general safety requirement for any product put on the market for consumers or likely to be used by them. The legislation requires that products are safe, and that producers provide consumers with the relevant information enabling them to assess the risks inherent in the product, particularly when they are not obvious, and take appropriate actions to avoid these risks (withdrawal from the market, warning to the market consumers, recall products already supplied…).

RECOMMENDATION 2: PRODUCT SAFETY

Although most of the legislation is well known to anyone operating in the business world, it is fair to say that eHealth products are still rather new and therefore little legal guidance exists on, for example, the type of information that is necessary and relevant to allow a purchaser to assess the risks of using a product.

However, national authorities have been established to monitor product safety and to take appropriate measures to protect consumers. An information system has been put in place that imposes collaboration between distributors, producers and the national authorities but also between Member States and the European Commission (RAPEX).

It would seem that at present this system is not well used for eHealth products. Accordingly, the European Commission should adopt policy tools to encourage the use of the RAPEX system for eHealth products.

ISSUE 3: MEDICAL DEVICES

According to the Directive 93/42 on Medical Devices, a 'medical device' is any instrument, apparatus, appliance, material or other article, whether used alone or in combination, including the software necessary for its proper application intended by the manufacturer to be used for human beings for the purpose of:

- diagnosis, prevention, monitoring, treatment or alleviation of disease;
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap;
- investigation, replacement or modification of the anatomy or of a physiological process;
- control of conception,

and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means.

The Directive requires that medical devices be designed and manufactured in such a way that their use do not compromise the safety and health of patients, users and other persons when properly installed, maintained and used in accordance with their intended purpose. When a

Member State notes that a medical device conforming to the Directive compromises the health and/or safety of patients, users or, where applicable, other persons, it must take all appropriate interim measures to withdraw such devices from the market or prohibit or restrict their being placed on the market or put into service.

Since electronic equipment and software is included in the definition of medical devices when they are manufactured or promoted for medical purpose, some eHealth products, such as monitoring devices, will be considered as medical devices under the European Medical Device legislation. However, eHealth tools used for the administration of general patient data will generally not be considered medical devices unless such a product (e.g., a PC, printer, screen, etc.) has had a specific medical purpose assigned to it.

RECOMMENDATION 3: MEDICAL DEVICES

More clarity is needed on the extent to which eHealth products are covered by Medical Devices legislation. Many of the currently available monitoring devices are covered only by general product liability, not by specific liability provision. It is suggested that further consultation on the application of medical devices legislation to eHealth tools takes place to establish if special guidelines should be issued.

ISSUE 4: LIABILITY FOR EHEALTH SERVICES

An eHealth service might be passive, such as delivering general medical information through a website, or might be active in giving medical advice or specific decision support to clinicians, or might involve the collection of biomedical data for remote monitoring by a clinician. Such a service might conceivably cause damage to someone relying on the service. A citizen might follow bad advice and fall ill, or even die; a clinician might follow the recommended procedure after using a decision support tool and might harm a patient; or a remote monitoring service might fail to transmit relevant data thereby putting a patient's life a risk.

There is currently no general European harmonisation of liability rules for services. Therefore, liability for services are governed by ordinary rules of contract law applicable in the Member States.

However, when an eHealth service is a purely technical one and the provider is an Internet intermediary who transmits or stores third party information, such as a web-based store-and-forward service for biosignal data for example, such a technical service provider will benefit from the rules of exoneration of liability established by the eCommerce Directive. These rules may minimise the risks for technical partners of eHealth service providers, who act as 'intermediaries'. Thus, web site hosting service will not be liable for the illegal sale of medical products made through an ePharmacy website.

RECOMMENDATION 4: LIABILITY FOR EHEALTH SERVICES

The European Commission should consider supporting the adoption of EU level guidelines that would seek to identify the various parties involved in delivering eHealth services and establish the various liabilities that each party must accept. Such guidelines should be widely disseminated in order to develop healthcare practitioner and patient confidence in the use of eHealth services.

In particular it should be investigated if specific guidelines on eHealth services could be drafted under the provisions for a Code of Conduct established in Directive 2000/31 on eCommerce.

Recommendations on Competition Law

The principles of free trade and competition are among the most important economic principles supported by the European Community. It is therefore not surprising the European Community has adopted a wide range of legislation to support competition through a legal system that prohibits any disloyal practices that restrict competition.

The core of European competition law is found in the rules applying to private firms or "undertakings" in articles 81 and 82. Article 81 prohibits agreements and concerted practices with an anticompetitive object or effect on the market, while Article 82 prohibits abuse of a dominant position. Furthermore, article 86(2) states that the rules on competition also apply to public undertakings as long as the "application of such rules does not obstruct the performance, in law or in fact, of the particular tasks assigned to them."

The law encapsulated in the key articles above, as well as a wide range of ECJ case law, is established to allow fair and open competition between undertakings operating in the European Union and with a potential effect on trade between the Member States.

ISSUE 1: UNDERTAKING – WHEN IS AN ORGANISATION ACTING AS AN UNDERTAKING?

The rules of competition law on abuse of dominant position and concerted practices are defined by the Treaty to apply only to those organisations classified as 'undertakings'. The key question for purposes of healthcare providers is therefore whether any of the parties to an eHealth service are deemed to be undertakings and therefore subject to competition law.

The recent case law at national and EU level has established that publicly funded health bodies may, in certain circumstances, be subject to competition law. However, the case law is unclear but would seem to provide that the same institution may, in some aspects of its conduct, be regarded as an undertaking (if it offers goods or services on the market) but in other aspects (such as contracting out certain care services) will not be considered an undertaking.

This ambiguity in law will be unsettling for both public and private sector healthcare providers. Suppliers to the public sector, such as remote monitoring service providers, may feel that they have been left defenceless against large public purchasers, such as a national health system. However, public buyers have equally been left on shaky ground, especially those competing with private operators in the provision of goods and services.

RECOMMENDATION 1: CLARIFICATION OF THE LAW ON UNDERTAKINGS

The appropriate committees of the European Commission should be encouraged to examine the recent decisions of the ECJ on the application of articles 81 and 82 to healthcare providers in order to draw up clear guidelines establishing when a healthcare provider will be regarded as an undertaking and when not.

Such guidelines should address the widest possible range of healthcare providers and suppliers, covering traditional and eHealth care.

ISSUE 2: HEALTH SERVICES AS SSGI AND/OR SGEI

The Treaty provides that an undertaking normally subject to the rules of competition law may be exempted from their application if it has been entrusted by a public body to provide a Service of General Economic Interest (SGEI) and if the application of the rules on competition would obstruct the performance of the particular tasks assigned to them. While it is left up to Member States to define the services they consider as SGEI, considerable lack of clarity still exists at EU level on the designation of health services.

Recognising that many European health systems are provided through public funds, the European Commission has, in a number of communications, suggested that health services are not generally to be regarded as SGEI nor are they to be included in the wider definitions of Services of General Interest or Social Services of General Interest. The Commission has instead proposed that, because health services have such a unique character, special targeted rules on health services (of general interest) should be established. However, despite first raising this issue in 2001, the European Commission has yet to clarify the position of health services and their possible exemption from competition law.

RECOMMENDATION 2: SPECIFIC CLARIFICATION OF HEALTH SERVICES WITH RESPECT TO SGEI

It is recommended that the Commission adopt a communication or guidelines that set out clearly the circumstances under which a health service provider may make use of the provisions on SGEI in the Treaty and thus be exempted from competition law. Such guidelines should address the changing nature of health services, recognising that a wide range of actors from both public and private enterprises will be involved in the provision of both traditional and eHealth services. In order to encourage adequate investment in eHealth services, both public and private enterprises must have legal certainty on their position with respect to competition law.

Recommendation on dissemination of legal knowledge

eHealth products and services raise numerous new legal questions. Among these, the "Legally eHealth" study has examined in particular data protection, liability and consumer protection, and some aspects of competition law as being the most prominent. The results of the study have shown that European law provides the Member States with a significant number of harmonised answers and solutions regarding these topics.

However, presentation of the study at various conferences and meetings has revealed that there is a lack of legal knowledge necessary to support the development and uptake of eHealth products and services. In other words, patients, medical practitioners, entrepreneurs, policy-makers, and others are not fully aware of the legal context in which eHealth products and services can and should be deployed.

ISSUE: LACK OF KNOWLEDGE OF EHEALTH LAW

The European Commission already supports various efforts to disseminate knowledge on information technology related law across the European Union, notably the LEFIS

Thematic Network[9] which seeks to develop, implement and consolidate a cross-national teaching and research infrastructure to respond to the needs and problems raised by the information and knowledge society.

RECOMMENDATION: DISSEMINATING KNOWLEDGE ON EHEALTH LAW

The European Commission should consider supporting a targeted tool for the dissemination of legal knowledge relative to eHealth products and services. As well as providing a repository of shared teaching material such as the LEFIS Thematic Network, this could:

- support the development European guidelines based on real cases;
- encourage the study of legal norms and rules applicable to eHealth products and services;
- promote public information on legal norms and rules applicable about eHealth products and services.

It is also worth noting that some other legal disciplines have started to establish successful virtual "European universities". A good example is the French association ARFDM (Association de Recherche et de Formation en Droit Médical) which, in collaboration with the Paul Sabatier University (France, Toulouse) and many other European Universities as well as two major Canadian universities, organises a European Summer School on Medical Law. The first summer school took place in 2006 in Toulouse during the 16th World Congress on Medical Law and brought together 44 field specialists. A second session is due to take place in 2007 in Madrid.

This kind of approach is an ideal format for disseminating legal knowledge and especially legal knowledge about European rules applicable to the healthcare sector. During the summer school, teachings focus on the basis of European medical law.

It is recommended that the European Commission explore possibilities for supporting such summer schools dedicated to eHealth, in which clinicians and informaticians would have the opportunity to share information and learning not only on technological advances but also on legal complexities.

Deleted: similar

Recommendation on an eHealth information infrastructure guidelines

When eHealth services, such as electronic health records, first began to be provided by traditional healthcare providers such as hospitals and general practitioners, such products and services were supported by specifically dedicated telematic infrastructures (closed circuits and intranets), such as for example the MammoGrid infrastructure[10].

Today however, we are witnessing a new phase of eHealth in which numerous projects aim to exploit the existing information highway, the Internet, for linking disparate healthcare providers for occasional, ad hoc as well as pre-defined networking.

[9] http://www.lefis.org/

[10] http://www.gridstart.org/MAMMOGRID.shtml

The use of such web-based applications is, however, creating a need for a permanent eHealth informatics infrastructure that can support any kind of eHealth products or services, and that will lead eventually to a dedicated "Health Information Highway".

The establishment of a dedicated Health Information Highway has many challenges, including in particular the challenge of interoperability between systems and applications and a service oriented architecture (SOA) that can accommodate a wide number of dispersed applications in a field where the number of such applications is growing daily. Such architecture use can loosely coupled with devices to support the requirements of business processes and users, in an environment where services are made available as independent applications that can be accessed without knowledge of their underlying platform implementation. This approach has gained good support in the health sector not least because it also provides greater interoperability and some protection from lock-in to proprietary vendor software.

By definition, healthcare is an extremely fluid industry. Doctors, hospitals, insurance companies, and patients are subject to a never-ending series of regulatory changes, advances in treatment, procedural changes, and mergers and acquisitions. Each change requires an adaptation of systems, and each adaptation potentially impacts some or all systems. Point-to-point integration quickly becomes costly and complex to maintain, and results in delays, inaccuracies, mountains of paperwork, and frustration for healthcare providers and consumers alike. The value of a SOA to the healthcare industry is that it enables health IT systems to speak the same language. If all systems can communicate using a common SOA framework, integration becomes less complex and IT can adapt to systems more rapidly.

Presenting a powerful argument for SOA in health, Greg Mummah argued in an article in the *Business Integration Journal* that "SOA can provide the building blocks that help healthcare-related IT organizations improve patient treatment and billing. It enables IT to focus on process improvement by removing system-to-system communication headaches. It makes organizations more adaptable to change"[11].

The challenges with the SOA and the adoption of a Health Information Highway are predominantly technical: interoperability and security remain huge challenges, which are being actively tackled by a number of European and national initiatives. However, the challenges are not purely technical. The adoption of such technologies also requires that the legal framework be properly adapted to the use of multiple applications by distributed actors.

Although work on health information highways has been started in many Member States, it is questionable in how far these networks are fully compliant with Directive 95/46/EC on Data Protection and how much these different highways might lead to an interoperable international highway.

ISSUE: HEALTH DATA PROCESSING REQUIRES FINALITY OF PURPOSE

At present each Member State has to draft specific legislation within the constraints of its duties within EU level Data Protection law. It is therefore suggested that the development

[11] Greg Mummah; "SOA Cures Healthcare Integration Headaches" in *Business Integration Journal*. Accessed at http://www.bijonline.com/index.cfm?section=article&aid=229# on 14th January 2007

and uptake of such network infrastructure could be greatly speeded up and much aided by specific EU level legislation that would set out harmonised rules for the free circulation of data within such a network infrastructure.

The concept of such targeted data protection legislation is not new, as seen in Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector. It is argued therefore that an important next step for the legal clarification of eHealth would be taken in the adoption of a similar Directive (or a Recommendation) taking into account the characteristics of the underlying infrastructure supporting eHealth products and services.

RECOMMENDATION: A DIRECTIVE OR CODE OF CONDUCT ON PRIVACY AND HEALTH INFORMATION INFRASTRUCTURE

A suggested Directive or Code of Conduct on Privacy and Health Information Infrastructure should be developed within the context Directive 95/46/EC and could take the form of either a dedicated Directive or could be an EU-level Code of Conduct to be approved by the European Working Part on Data Protection set up under article 29 of the Directive. Any such Directive or Code would be complementary to Directive 95/46/EC on Data Protection and Directive 2002/58/EC on Privacy and Electronic Commutations.

The suggested Directive or Recommendation should include the following key elements:

- define the actors involved in health information systems and their duties and rights; with respect to this, all activities within a Health Information Infrastructure should be monitored by a personal data protection official;
- define security requirements for both the infrastructure and the eHealth products and services;
- ensure the confidentiality of the personal data transiting through the infrastructure and through the eHealth products and services;
- address the question of the use of the traffic data and other location data;
- regulate the directories or registries required for the creation and the operating of the infrastructure and of the eHealth products and services (management of medical practitioners' and patients' personal data);
- regulate the interoperability of the infrastructure and of eHealth products and services;
- provide auditing measures;
- provide special supervisory authorities at local, national and European levels considering the size of the information system;
- describe the prior checking to take place before the operating of the infrastructure and of its products and services.

The suggested Directive or Recommendation should also determine precisely:

- the possible bases of legitimacy other than the data subject's consent to create the infrastructure of those new information systems in healthcare, notably in terms of individual or collective benefits for the patient and for the community (guaranteed access to treatment, diagnosis, medicine, etc.) especially where private companies will be using these information systems to produce new scientific knowledge;

- the appropriate safeguards required to allow for the further processing of personal data (and especially of medical data) for substantial public interests (without requiring the data subject's consent) like scientific research (example of appropriate safeguard: a first coding by the initial data controller and a second coding by a trusted third party gathering all the data from the data controllers before sending them to the researchers);
- the appropriate safeguards allowing for keeping the data for longer periods for scientific use;
- the terms under which identification numbers or other identifiers may be used;
- the exact consequences of the compliance with these safeguards notably in terms of data subject's information and rights (to access, to rectify, to oppose, etc.);
- the creation of effective judicial remedies, providing for compensation in case of breach of rules and for effective and dissuasive criminal sanctions;
- the terms under which (coded) personal data may be transferred to third countries for scientific research.

Although it may, of course, be decided that the time is not right for the adoption of a Directive dedicated to privacy in eHealth, it is recommended that at the very least a thorough investigation be undertaken on the way in which a select number of national health systems are currently addressing the issues outlined in the key points above, in order that a solid case for at least national level responses to the issues may be made.

It should be noted, moreover, that the purpose of such a study would be not only to establish the need for EU level health data protection harmonisation, but would also provide a solid basis for the establishment of harmonised approaches to cross-border healthcare in a context in which, at present, no simple Treaty-based legitimation is available.

Final Point: Impact Assessment on all future policy and Legislation for eHealth

The "Legally eHealth" study has examined aspects of European law related to data protection, liability and consumer protection, and competition law. It has identified that a significant body of European law already addresses a number of the key legal issues in eHealth, even if not directly so. Data protection, for example, looks at the special needs of health data whilst recent changes to the medical devices directives examine the role of software within medical devices. It has been noted also that recent case law recognises that some aspects of competition law may apply to public and private enterprises operating in health and eHealth service provision.

However, it is notable that despite the large numbers of communications on Services of General Interest, the Lisbon agenda and long-term care, as well as heated debates on health services with the Services Directive, little emphasis has been given to an impact assessment of the proposed legislative responses to health services in general and none have considered in depth their impact on eHealth services. Given however that the development of eHealth markets have been considered, for example by the Aho Report, as a major potential economic activity for Europe, further legal clarifications are necessary both to encourage the

development of these markets in optimal conditions all the while respecting the unique nature of health services.

eHealth is important for Europe: it can drive up service quality, improve patient safety, contain costs and facilitate access to healthcare. However, there is still great uncertainty in the eHealth actors, ranging across public bodies, big industry and small enterprises about the full legal implication of using and offering eHealth services.

The "Legally eHealth" study has shown that a significant body of law already exists and is well adapted to responding to many of the questions raised by using and providing eHealth services. However, to drive up market confidence these issues must be made more clear to all users, not only through dissemination work, but also by focussed impact assessment which will highlight the eHealth aspects of future policy and legislation in order that such legislation is properly adapted to the needs of this sector.

The final recommendation of the study is therefore to call for a mainstreaming of eHealth impact assessment across all European policy initiatives.