International Journal of Technology Assessment in Health Care, **20:4** (2004), 498–508.

Information technology law and health systems in the European Union

Elias Mossialos
Sarah Thomson
Annemarie Ter Linden
London School of Economics and Political Science

Objectives: This study aims to examine the impact of European Union (EU) law relating to information technology (IT) on health systems.
Methods: The study identifies EU directives relating to IT, analyzes them in terms of their impact on the use of IT in health systems, and outlines their implications for health technology assessment (HTA). Analysis is based on a review of literature identified through relevant databases and Internet searches.
Results: Developments in IT have serious implications for EU health systems, presenting policy makers with new challenges. The European Commission has adopted a range of legal measures to protect consumers in the "information society" However, as few of them are health-specific, it is not evident that they have implications for health, health systems, or HTA, and they may not be effective in protecting consumers in the health sector.
Conclusions: In light of the growing importance of IT in the health sector, legal and nonlegal measures need to be further developed at EU and international level. Where possible, future initiatives should pay attention to the particular characteristics of health goods and services and health systems. Although definitions of HTA usually recognize the importance of evaluating both the indirect, unintended consequences of health technologies and the legal aspects of their application, it seems that, in practice, HTA often overlooks or underestimates legislative matters. Those involved in HTA should be aware of the legal implications of using IT to provide health goods and services and compile, store, transfer, and disseminate health information electronically.

Keywords: Health technology assessment, Legislation, Europe, Internet, Medical informatics

It is not always evident that developments in information technologies (IT) may be of relevance to the field of health technology assessment (HTA), just as it is not immediately obvious that European Union (EU) legislation concerning IT may have serious implications for health and health systems. However, it is easier to see how developments in IT may affect health and health care. The rise of "electronic" health (e-health or telemedicine) and the proliferation of health-related Web sites on the Internet are likely to enhance European consumers' access to health care and information about health, as well as bringing potential benefits to health-care providers. At the same time, the introduction and diffusion of these health technologies present policy makers with new legal challenges, triggering both legal and nonlegal initiatives at national, EU, and international levels.

Over the past 20 years, the European Commission has promoted the development of IT within the EU, seeing it as an opportunity to create jobs and provide services more efficiently (33). Health and health care form a key part of the Commission's vision of an "information society" in which a new generation of computerized clinical systems, advanced telemedicine services, and health network applications will

Table 1. Selected European Community Legal Measures, in the Form of Directives, With Potential Consequences for e-Health

Date	Directive	Title
1985	85/374/EEC	Liability for defective products
1993	93/42/EEC	Medical devices
1995	95/46/EC	Protection of individuals with regard to the processing of personal data and on the free movement of such data
1996	96/9/EC	Legal protection of databases
1997	97/7/EC	Protection of consumers in respect of distance contracts
1999	1999/93/EC	A community framework for electronic signatures
2000	2000/31/EC	Certain legal aspects of information society services, in particular electronic commerce, in the internal market
2001	2001/95/EC	General product safety
2002	2002/58/EC	Privacy and electronic communications (repealing Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector)

improve health, continuity of care, health service management and intelligent systems, provide support to health professionals, and allow citizens to be more involved in and assume greater responsibility for their own health (29). For example, recent Commission initiatives—the eEurope Action Plans for 2002 and 2005—have focused on extending Internet connectivity throughout Europe, particularly in the area of health, and stimulating the spread of electronic health cards, health information networks, and online health services (28;33). The Commission has also adopted a range of legal measures to address issues arising from developments in IT (see Table 1).

In contrast to the eEurope Action Plans, many of the Commission's directives are not specific to health, although some do make reference to health-related issues. Consequently, it is not self-evident that they may have implications for health and health systems. However, closer examination of the substance of these directives reveals that they do affect health care, either directly or indirectly—the latter in so far as they affect health databases, Web site operators, and providers of telemedical services (see Table 2).

Definitions of HTA recognize the importance of evaluating both the indirect, unintended consequences of health technologies and the legal aspects of their application (7;41). Nevertheless, while such definitions clearly acknowledge the existence of legal implications, it seems that, in practice, legislative matters are often overlooked or underestimated in HTA.

This study takes the view that those involved in HTA should be aware of the legal implications of using IT to provide health goods and services and compile, store, transfer, and disseminate health information electronically. For example, as the use of IT in the health sector becomes more widespread, it seems appropriate for those concerned with evaluation to consider legal issues concerning product safety and security in electronic information transfers and financial transactions. In addition, legal initiatives regarding data protection, data ownership and intellectual property rights will have implications for those carrying out research, trials, and cost-effectiveness analyses. Finally, although the context is one of legislation, and the issues therefore appear to be predominantly legal in nature, they may also have medical, economic, social, and ethical implications.

Table 2. Legal Issues Relevant to Health or Health Systems

Relevance	Legal issue
Direct	The privacy of identifiable health data in electronic form held in databases or transferred through online networks, particularly maintaining confidentiality and ensuring data protection
	Tort-based liability
	Product safety
	The reliability and quality of information about health and health care provided electronically, mainly through health-related Web sites
Indirect	Ownership and intellectual property rights
	The security of information transferred electronically (electronic signatures)
	The security of electronic financial transactions (electronic commerce and consumer protection in distance selling)

The study aims to examine the directives outlined in Table 1 and show how they affect the use of IT in EU health systems. Each of the following sections begins by describing the relevant directives and discusses issues arising from them, with examples of actual cases where possible. The study does not discuss the implications of the Commission's nonlegal initiatives relating to IT, wider issues related to EU competition law, or issues related to medical devices or quality assurance in e-health. These issues are discussed in some detail in Vajda and Gahnström (57), Altenstetter (2), Terry (50), and Eysenbach et al. (32).

DATA PROTECTION

Confidentiality is vital to any medical exchange. Where confidentiality between professionals and patients is not guaranteed, the latter could face psychological barriers to seeking care. Rapid developments in IT necessitate new safeguards. To ensure confidentiality in electronic exchanges, computer and telecommunications systems must be secure, all those who handle information must have a high duty of confidentiality, and patients must have the opportunity to verify any information that is held about them (61). The Commission has adopted two directives to ensure confidentiality in processing data, although some remain pessimistic about the

extent to which privacy can be guaranteed in the information society (44). Others argue that the push to promote electronic commerce has been an important catalyst in the drive toward comprehensive legislation on data protection (38).

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data—known as the Data Protection Directive—aims to protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy with respect to the processing of personal data (Article 1.1) (21). It also aims to harmonize data protection legislation to facilitate the free flow of personal data between EU member states (Article 1.2) (1). Protection should be provided at the highest standard available under national law within the EU rather than being based on average standards of national protection (13).

Building on the principles enshrined in the Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the Directive applies to all data, including manually held records containing personal information (14;48). Personal data are defined as any information on an identified or identifiable natural person, irrespective of whether that person is directly or indirectly identified. The Directive does not apply, however, to data collected for "purely personal" or "household purposes" (Article 3.2). For example, the personal notes of a physician might be regarded as purely personal but would cease to be personal if they were shown to the patient or to colleagues, at which point they would become subject to the Directive.

Organizations processing data must appoint a "data controller"—either a person or a body to determine why and how data are to be processed—and register the controller with the public authority (Article 28). With regard to the health sector, the data controller might be a professional or a health authority. Data must be processed fairly and lawfully; collected for specified, explicit, and legitimate purposes; and not further processed in a way incompatible with those purposes. Data are also required to be accurate, relevant, kept up to date where necessary, and not excessive given the purposes for which they are stored. The principle that data should be kept up to date where necessary suggests that the obligation is not compulsory. For example, a physician must regularly confirm that a patient's address is correct but not during every contact with the patient. Additionally, data should be kept in a form that permits the identification of individual data subjects only for as long as necessary and for the purposes for which the data were originally collected (Article 6).

The processing of personal data requires legitimate grounds for processing. In most cases relating to health care, personal data may only be processed if it is necessary for the execution of a contract to comply with a legal obligation, to protect a patient's vital interests, or if the patient has unambiguously given his/her consent (Article 7). For example, in the Netherlands, a patient's medical data can be processed for the execution of a medical treatment contract.

Article 12 notes that individuals have a basic right to verify and correct their personal information. The sensitivity of personal health data is recognized in Article 8, regarding the processing of "special categories" of data, which is prohibited unless safeguards are in place (1). Special categories include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or disclosing details of a person's health or sexual orientation. Although the Directive identifies health data as a special category and generally prohibits their processing unless an individual has given explicit consent, there are exemptions to this under certain situations, for example when it is necessary to protect the interests of individuals who are physically or legally incapable of giving consent (43). According to Article 17, appropriate technical and organizational measures have to be taken to ensure the security of stored data. Technical measures include passwords, back ups, and privacy-enhancing technologies, while organizational measures encompass the partition of responsibilities and authorities. Article 25 restricts the transfer of personal data outside the EU, except where third countries guarantee "an adequate level of protection," as judged by the standards of the Directive.

The Directive raises several issues that require further clarification. These include what constitutes data processing, uncertainty about the nature of the data controller, the appropriate technical and organizational measures that need to be taken to ensure the security of stored data, the transfer of data to third countries, and the degree of harmonization achieved.

In response to the Directive, member states have established an independent public authority to supervise personal data protection. However, in the United Kingdom, the Court of Appeal and the independent public authority have given different interpretations of what constitutes data processing, the latter arguing that anonymizing personal data amounts to processing data (59). The regulatory consequences of such an interpretation are that anonymization will need to comply with the Directives' principles, particularly the principle concerning fair and lawful processing. Walden notes that this compliance would require notifying the data subject that such a process was to be carried out, giving rise to the concern that strict compliance with the Directive could discourage the adoption of privacy-enhancing procedures such as anonymization.

Although the Directive provides for patients' rights to privacy and the appointment of a data controller to oversee the processing of data, the question arises as to who this might be in organizations with complex structures and shared responsibilities. It is clear, for example, that a general practitioner (GP) who manages his/her own practice will be responsible for data processing, whereas the responsibility will be collective in group practices. In the case of hospitals and consultant physicians, the hospital will be the main data

controller and consultants will only be partially responsible. However, where increased data flows require the involvement of GPs, consultants, hospitals, and health authorities, the division of responsibilities is much less clear, which could lead to problems for patients (35).

At the same time, questions arise as to what type of technical and organizational measure to protect stored data might be considered "appropriate." Recital 46 states that "appropriateness" depends on the state of the art and the cost of implementation in relation to the risks inherent in the processing and nature of the data to be protected. However, this clarification seems vague, particularly because some health data may have significant commercial value for third parties, such as insurance companies and the pharmaceutical industry (45). The Council of Europe Recommendation R (97) 5 on the protection of medical data gives greater health-relevant guidance on security measures, including control of entrances to installations, data media, memory, utilization, access, communication, data introduction, transport, and availability (Article 9), but Council recommendations are not legally binding (61).

The transfer of data to third countries has been problematic. While countries such as Canada responded to the Directive by adopting their own national privacy legislation, countries such as the United States failed to meet the EU standard for adequate data protection, posing potential difficulties for U.S. businesses with EU operations—for example, U.S. pharmaceutical companies needing data from European clinical trials for scientific research (6;16;38). U.S. companies either had to absorb the additional costs of meeting the EU standard or risk losing access to information about EU citizens (38). In 2000, the U.S. Department of Commerce reached an agreement with the EU on a "Safe Harbor Framework" to allow individual organizations to operate on the basis of a system that certifies their provision of adequate data protection as defined by Article 25 (55). The Department maintains a list of self-certified organizations but does not guarantee its accuracy or assume liability for it; therefore, while EU officials consider the safe harbor framework to be a useful tool, differences between the United States and the EU remain (38;54;53). Nevertheless, Long and Pang Quek suggest that the Directive was instrumental in pushing the United States to reconsider its privacy arrangements (38). In April 2003, the first U.S. federal privacy standards to protect patients' medical records and other health information held by health-care providers came into force (56). These new regulations limit the ways in which health insurers, pharmacies, hospitals, and other entities can use patients' personal medical information, such as medical records and other individually identifiable information, whether it is held in computers, on paper, or communicated orally.

Finally, some have questioned the degree of harmonization of member states' policies and practices achieved by the Directive, because the Directive gives member states considerable scope for derogation and does not apply to the processing of personal data in the course of any activity that falls outside the scope of EU law, although this scope has not been defined by the Directive (13). Article 8.4 provides an example of the degree of dissonance that exists, as it is not specific to the processing of medical data for research purposes. On the basis of this article, member states have to provide exemptions to the prohibition of processing medical data for reasons of substantial public interest concerning the provision of suitable safeguards. As a result, there is no guarantee of harmonized legislation, even though the use of medical data for research purposes often requires the transfer of data from one member state to another (8).

In July 2003, the Commission's regulatory framework for electronic communications came into force. It comprises a framework directive (2002/21/EC) and four directives covering authorizations (2002/20/EC), universal service (2002/22/EC), access and interconnection (2002/19/EC), and data protection and privacy in electronic communications (2002/58/EC) (the ePrivacy Directive). The ePrivacy Directive replaces Directive 97/66/EC—which was established to regulate privacy in telecommunications and extended certain privacy rights to legal as well as natural persons—with effect from 31 October 2003 (61). Directive 97/66/EC applied to the processing of data in connection with the provision of telecommunications services in public telecommunications networks, in particular by means of integrated services digital networks (ISDN) and public digital mobile networks (Article 3.1). The new framework governs all electronic communications services and replaces existing telecommunications regulations (24).

Some aspects of the ePrivacy Directive require additional clarification, particularly as electronic communications services are defined as services provided for remuneration. Internet providers that provide free access, therefore, may not fall within the scope of the Directive, because they do not receive remuneration—or at least financial compensation—from Internet users. However, in dealing with services in the sense of Article 50 of the EC Treaty, the jurisprudence of the European Court of Justice (ECJ) suggests that this interpretation may not be valid because remuneration can be paid by a third party, such as advertisers, rather than the recipient of the service (ECJ Case C-109/92: Stephan Max Wirth v Landeshauptstadt Hannover).

OWNERSHIP OF DATA AND INTELLECTUAL PROPERTY RIGHTS

As noted above, the Data Protection Directive stipulates that data should only be processed for specified, explicit, and legitimate purposes but permits further data processing for scientific research purposes in the area of health care if it can be justified on grounds of substantial public interest, even if not originally declared to the data subject, so long as appropriate care to ensure confidentiality is taken (Recital 34). However, when medical data cannot be directly or indirectly

related to any identifiable person, the question arises as to who owns this information (61).

Directive 96/9/EC on the legal protection of databases attempts to address this issue of ownership by improving the previously weak copyright protection for databases (22). The Directive defines a database as a collection of independent works, data, or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means (Article 1.2). It may protect commercially valuable information gathered by electronic commerce businesses, such as consumer lists, product lists, and electronic directories (37).

There are two types of database protection: copyright and sui generis right. The former applies if, by reason of the selection or arrangement of the database contents, there is an intellectual creation by the author (Article 3.1); this intellectual creation must be original. The latter applies if the database has not been intellectually created by selection or arrangement, like many medical databases, which are mostly a comprehensive listing of factual data (61). The sui generis right also suggests that there has been—qualitatively and/or quantitatively—a substantial investment in either the obtaining, verification, or presentation of the contents of a database to prevent extraction and/or re-utilization of the whole or of a substantial part of the contents of that database (Article 7.1). It expires 15 years from the first of January of the date of the completion of the database (Article 10.1). According to Article 9, exceptions to the sui generis right are possible: extraction or re-utilization of the content of a database may take place without the authorization of its maker. Paragraph b of Article 9 may apply to the health sector: extraction may take place for the purposes of illustration for teaching or scientific research, as long as the source is indicated, and to the extent justified by the noncommercial purpose to be achieved.

It is argued that the Directive effectively sets the global agenda for national and international database protection, going beyond the protection afforded to databases in other areas of the world, notably the United States (51). However, it is not entirely clear to what extent this level increases the protection available to owners of health-related databases. Thakur (51) points out weaknesses in the Directive, arguing that it fails in several respects to qualify as an optimum global model.

First, the Directive does not define "substantial investment" in the sui generis right. It is not clear whether the investment involves time, effort, financial resources, or a combination of these, although it is likely that the certainty of database protection will increase if the investment of human and financial resources is greater.

Second, there is uncertainty about the degree of harmonization that can be achieved by the Directive. According to Recital 52, Nordic countries can apply the exception or exclusion of official documents, in respect of the sui generis right, under their "catalogue rule." Protection of nonoriginal and nonindividual databases is only granted when the catalogue consists of a large amount of information—for example, telephone catalogues or large health databases (49). Small health databases are excluded, even if their construction required substantial investment (49). If the Nordic countries take advantage of this position, differences in legislation will arise within the EU.

Finally, the Directive has created considerable imbalance in the legal protection of databases between EU member states and third countries. The United States, for example, applies database protection to the format but not the content of a database, whereas the EU Directive protects both. Lack of harmonization and the imbalance between EU member states and third countries may be detrimental to the production of valuable databases for the promotion of health research and science (51).

ELECTRONIC SIGNATURES

An electronic signature is a generic technology-neutral term covering the methods by which electronic records can be signed. It may exist in a variety of forms and can be created by different technologies (10). The electronic signature is a key tool in ensuring confidentiality, integrity, and authenticity in the transfer of health data between electronic sources (1;61). It is vital, therefore, for building patient confidence in and maximizing the opportunities presented by electronic commerce (45).

Although a wide range of electronic signature tools exist and are extensively used, electronic signatures were not widely legally recognized within the EU before the introduction of Directive 99/93/EC on a Community framework for electronic signatures. This Directive aims to establish a legal framework for electronic signatures to create a homogenous, technology neutral background for the operation of electronic signatures issued through certification service providers (CSPs) anywhere in the EU (Article 1) (25). A CSP is an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures (Article 2.11). Examples of relevant services include registration, computing, directory, or consultancy services (Recital 9).

Article 3.7 of the Directive states that member states may make additional requirements for the use of electronic signatures in the health sector. Conditions for such requirements should be objective, transparent, proportionate, and nondiscriminatory and should relate only to the specific characteristics of the application concerned. Furthermore, any additional requirements should not be a barrier for patients that use health services abroad.

To ensure the proper functioning of the internal market, member states may not restrict the provision of certification services originating in another member state (Article 4.1). The Directive also requires member states to ensure that CSPs are liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate

(Article 6). Interoperability at the international level is ensured through mutual recognition of certification services originating in third countries, so long as the CSP (40): fulfills the requirements of the Directive and has been accredited under a voluntary accreditation in a member state; is guaranteed by a CSP established and accredited within the EU; or is recognized under a bilateral agreement between the EU and third countries or international organizations (Article 7.1).

To facilitate cross-border certification services, the Commission can make proposals, where appropriate, to achieve the effective implementation of standards and international agreements that will be decided by qualified majority of the Council (Article 7.2). The Commission also emphasizes the importance of CSPs observing data protection legislation and individual privacy in compliance with the Data Protection Directive, so as to increase user confidence in electronic communication and electronic commerce (Recital 24).

As with the directives discussed above, concerns about the Electronic Signatures Directive focus on harmonization. The Directive recognizes two types of electronic signatures: a simple electronic signature and an advanced electronic signature based on "a qualified certificate and created by a secure-signature-creation device" (Article 5). Both types of electronic signature cannot be denied legal effectiveness and admissibility as evidence in legal proceedings solely on that grounds that they are in electronic form. A certified signature is legally equivalent to a hand-written signature and is consequently admissible as evidence in legal proceedings. Because the liability rules of Article 6 only apply to advanced electronic signatures, the governance of the producers of simple electronic signatures falls under national liability rules. Consequently, there is no harmonization for electronic service providers within the EU (9).

Furthermore, the Directive does not provide a basis for dealing with electronic, as opposed to paper, documents. Further legislation is necessary to allow electronically signed documents to be treated in exactly the same way as paper documents. Specifically, some national laws still require certain health-related documents, such as prescriptions, to be produced on paper. Because the Directive does not cover the conclusion of contracts or other noncontractual acts (Article 1), member states are not required to address these issues (61). Despite this finding, the use of electronic prescriptions is acceptable in Finland, Sweden, and Denmark, while several other member states are carrying out pilot projects involving electronic prescriptions (39).

Finally, the legal issues regarding electronic signatures largely fall on health-care providers rather than telecommunication service providers. It is argued that, if the liability of the telecommunication service provider were to increase, the telecommunication service costs would be much higher. As a result, lower costs are at the expense of patients' rights to compensation (61).

CONSUMER PROTECTION IN DISTANCE SELLING

EU Directive 97/7/EC on the protection of consumers in respect of distance contracts is the EU's key legal text applicable to contracts concluded at a distance. It seeks to protect consumers—as natural persons and not in a commercial or professional capacity (Article 2.2)—from the risks that may arise when they are unable to examine goods before purchase or to check the supplier's premises (Article 2.3), as is often the case with telemedicine and use of the Internet (23).

In the health sector, the supplier will usually be a health professional, a health authority, or a company such as a pharmacy. Suppliers are required to comply with the duties outlined in the Directive in situations where they use one or more means of distance communication to conclude a contract. One of these duties is the consumer's right to written information about the identity and address of the supplier; the main characteristics and prices of the goods or services including taxes; the arrangements for payment, delivery, or performance; and the right of withdrawal. Where a written document is not foreseeable, the information has to be given in another durable medium, such as a CD-ROM but not an email (Article 5.1). The consumer also has a right to withdraw from the contract, within a period of at least 7 working days from the time at which the written information is supplied, without penalty and without giving any reason (Article 6.1). Unless specified otherwise, the supplier has to perform the order within a maximum of 30 days from the day after that on which the consumer forwarded his/her order to the supplier (Article 7.1).

One issue in interpreting the Directive relates to the difficulty of distinguishing between the consumer defined as a person acting "outside his [sic] trade, business or profession" (Article 2.2) and the supplier identified as acting "in his [sic] commercial or professional capacity" (Article 2.3). Although the Directive attempts to emphasize the status of the supplier as a knowledgeable specialist in comparison to the consumer, the latter may sometimes be more of an expert than the supplier or the supplier may not be suitably qualified. Furthermore, the sale on the site should be business-to-customer and not business-to-business, which involves different rights (34).

Another issue concerns the fact that, although the supplier is required to describe the main characteristics of the goods or services for sale, the complexity of health information and the challenge of judging its applicability in different circumstances could mean that few consumers have the specialized knowledge needed to interpret the health information on offer. The distance between the supplier and the consumer can make it harder for the consumer to ask for further clarification.

A third issue is that, as the supplier may not request any medical information from the consumer before selling a

product, consumers may have unsupervised access to potentially dangerous products. Several studies confirm the existence of irresponsible suppliers (4;5;31).

The Directive requires member states to implement a minimum level of consumer protection, but also allows them to introduce more stringent provisions so long as they are compatible with the Treaty (Article 14). However, to the extent that inconsistent regulations applying to distance communications hinder the conduct of online commerce, they may be incompatible with the free movement of goods and services guaranteed by the Treaty and may therefore be inconsistent with the Directive (46). In a recent ruling—the DocMorris case—the European Court of Justice decided that a national prohibition on the sale of drugs by mail order contravenes EU law where it applies to nonprescription drugs that have been authorized for sale in that country (30). The Court further noted that a prohibition on the sale of prescription only drugs by mail order would not contravene EU law, because the sale of such products could increase the risk of prescriptions being abused or incorrectly used. The latter decision may be irrelevant in member states such as Germany, where the government has already enacted legislation to permit online sales of prescription only drugs.

It could be argued that the Directive does not provide consumers with comprehensive protection, specifically because protection is only granted when contracts are concluded—and concluded at a distance—and does not apply to consumers merely surfing the Internet (47). In this respect, it is worth noting that health-related Web sites are among the most widely accessed Web sites on the Internet (60).

ELECTRONIC COMMERCE

Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market aims to enhance the free movement of information society services within the EU (Article 1) (26). These are services that are provided for remuneration and take place online and at the request of a recipient of a service. In the health sector, the recipient of a service can be a health professional or a patient. For example, the Directive may apply to the use of electronic cancer registries by physicians who pay a fee for accessing the data, the setting up of a Web site by a physician promoting his/her activities, or the online sale of pharmaceuticals (11). However, activities that cannot be carried out at a distance or by electronic means, such as physical examinations, are outside the scope of the Directive (Recital 18).

Article 3.1 states that each member state should ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in that member state that fall within the coordinated field. The coordinated field covers only requirements relating to online activities, for example online information and online shopping, but does not concern member states' legal requirements relating to goods, such as liability for goods, or requirements relating to the delivery or transport of goods (Recital 21).

According to Recital 19 of the Directive, the place of establishment of a company providing services by means of a Web site is not the place at which the technology supporting its Web site is located or the place at which its Web site is accessible, but the place where it pursues its main economic activity. This means that an agreement between a telephysician in Belgium and a consumer in the United Kingdom is most likely to be subject to Belgian law. However, according to Article 3.3 and the Annex—which follow from Article 3.1 of the Convention on the law applicable to contractual obligations (80/934/EEC)—both the telephysician and the consumer are free to choose the applicable law beforehand by agreement, although it is doubtful whether this happens in practice (11;18). Nevertheless, there are exceptions. A member state may take measures to restrict the freedom to provide information society services from another member state if the measures are necessary to protect consumers or public health.

The Directive complements the existing laws protecting consumers in the EU and concerns three areas: general information to be provided, commercial communications, and contracts. In terms of general information, the Directive goes beyond the Distance Selling Directive (see above) by requiring more information to be provided, particularly regarding prices and essential terms and conditions (Article 5).

For commercial communications, the new Directive also goes beyond the Distance Selling Directive in requiring the service provider to identify clearly the commercial nature of the communication, the person on whose behalf the communication is made and, where authorized, promotional offers such as discounts, premiums, gifts, competitions, and games (Article 6) (47).

According to Article 8, the telephysician may use commercial communications but he/she has to comply with the professional rules concerning, in particular, the independence, dignity, and honor of the profession, professional secrecy, and fairness toward clients and other members of the profession. However, codes of conduct at the EU level have not been developed as yet. Professional bodies and associations have to be encouraged to draw up or adapt codes of conduct at the EU level to determine the types of information that can be given for the purposes of commercial communication, to further the development of cross-border services (58). An example of professional regulation is the licensing system. However, a disadvantage of the licensing system is that it is not internationally approved. In the case of online health care, this means that a telephysician needs licenses in several jurisdictions and countries. It is unlikely that a specific license for telephysicians will be developed under the Directive, because Article 4.1 states that the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorization (11).

The Electronic Commerce Directive completes the Distance Selling Directive by defining exactly when a contract is concluded and by informing the recipients of the service of the procedure for correcting handling errors (Articles 10 and 11) (47). It also seeks to clarify the liability status of intermediary services providers, because uncertainty over their legal obligations in different jurisdictions has arisen in different cases. For example, a service provider acknowledged its liability for not removing Web site postings that were alleged to be defamatory in the United Kingdom, whereas in Germany a service provider was invalidated for failing to block access to child pornography (42).

According to Pearce and Platten (42), it is inconceivable that service providers should be both aware of and responsible for the entire content of their Web pages. The Directive provides liability limitations for three types of intermediary services providers. It does not contain the liability issue in the relationship between telephysician and patient (see the section on liability). A first exemption applies to service providers that are essentially passive or mere conduits of information to and from third parties (Article 12). A second exemption applies to "caching," when a service provider undertakes automatic, intermediate, and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request. The conditions for this exemption are, for example, that the provider does not modify the information and that he/she complies with conditions on information access (Article 13). The last exemption applies when the service provider does not have actual knowledge that the information stored at the request of the recipient of the service—"hosting"—is illegal (Article 14).

Although the Directive plays an important role in creating the legal framework for online health care, it is debatable whether consumers will rely on the courts and applicable rules of the country in which the telephysician is based when there is no contractual arrangement concerning applicable law (see above). According to Callens (11), a patient who does not live in the same country as the physician, being a consumer, deserves protection on the ground of mandatory rules of the law of the country of his/her normal residence. Besides, bearing in mind the specific nature of telemedical sessions, it may be possible for a consumer to prove, in conformity with Article 4.5 of the Rome Convention, that it ensues from the circumstances as a whole that the contract is more closely connected to the country in which he/she lives (18).

Another concern relates to codes of conduct. It remains to be seen whether codes of conduct to be drawn up at the EU level will cover current disparities in the level of protection for consumers using health services on the Internet (45).

PRODUCT SAFETY

One aspect of consumer protection involves preventing unsafe products from reaching the market. Directive 2001/95/EC on general product safety (GPS) expands the scope and impact of Directive 92/59/EEC on GPS (20;27). The 2001 Directive was made necessary by developments in product safety, together with changes made to the Treaty, particularly Article 152 concerning public health and Article 153 concerning consumer protection (Recital 1).

An evaluation of the 1992 Directive (12) shows that some member states have a higher level of consumer protection than the level defined by the Directive. The 1992 Directive had very limited impact in practice. This finding does not mean that unsafe consumer products were being placed on the market, but in most member states, the penalties that might be imposed in the case of failure to comply with the obligations had never or almost never been enforced. Furthermore, the evaluation shows that the preventive effect of the Directive on Product Liability (see below), such as fear of tarnishing a brand image or being sued for damages, is far greater than the penalties that might be imposed by the 1992 Directive (12).

The 2001 GPS defines a product as any product that is "intended for consumers or likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them, and is supplied or made available, whether for consideration or not, in the course of a commercial activity and whether new, used or reconditioned" (Article 2a). In the health sector, for example, the 2001 Directive applies to medical devices that have been bought online. However, the pharmaceutical sector is not covered by the 2001 Directive (17).

According to Article 2b, a safe product is any product that "under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation, and maintenance requirements, does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons." The 2001 Directive states that producers are obliged to place only safe products on the market (Article 3). For example, medical devices have to be tested before they can be sold. Furthermore, producers and distributors have to provide relevant information to consumers, so that consumers are able to assess the risks inherent in a product (Article 5). Also, the 2001 Directive states that member states have to establish authorities with necessary powers to ensure compliance with the above obligations (Article 6). In addition, an EU information network will be developed for the exchange of information on, for example, risk assessment (called Rapex) (Article 10).

Although the main terms of the 2001 Directive are roughly similar to the 1992 Directive, the obligations of producers and distributors has been increased and the authorities have more effective market surveillance and control mechanisms under the 2001 Directive. For example, producers have to keep a register of complaints about products and take steps to warn consumers of product risks (15;36).

Market surveillance is an important tool for the enforcement of EU legislation on product safety with regard to, inter alia, pharmaceuticals and medical devices. Furthermore, the 2001 Directive guarantees both a high level of protection for consumers and supports the free movement of goods in the internal market.

In the past, medical devices were regulated in France, Germany, and the United Kingdom, where lines between drugs and medical devices have never been suitably differentiated. Disagreements between representatives from services, businesses, and national authorities emerged regarding the pursuit of high-level EU legislation and harmonization of technical issues. Moreover, advances in biotechnology, such as tissue engineering and bone cement and fillers, have been blurring the lines between medicinal products and medical devices. Because organizational channels for enforcing compliance with EU directives and domestic vigilance systems differ between member states, further negotiations at the EU level will be needed to address these new issues as they evolve (3).

The safety of services is not included in the 2001 Directive, because the Commission intends to identify the needs, possibilities, and priorities for EU action on the safety of services and liability of service providers, with a view to presenting appropriate proposals (Recital 1). However, all member states have national legislation in place to ensure the safety of health services, particularly legislation securing licensing of qualified and trained medical personnel. At the same time, all these separate national legislations may have implications for the protection of patients. For example, an English physician who has been struck off of the register of the General Medical Council (GMC) in the United Kingdom is not prevented from continuing to practice in any other member state (52). As a result, English patients could obtain online treatment from an English physician who is not considered competent by the GMC. Whether the 2001 Directive will have a greater impact in practice than the 1992 Directive remains to be seen.

Liability

When the preventive measures mentioned above fail, resulting in incidents or accidents, victims will be allowed redress from the suppliers and producers of the goods and services involved (17). If, for example, a patient suffers harm because a consultant misses the results of a diagnosis sent to him/her by a general practitioner, the consultant will have been culpably negligent. But if the missed diagnosis took place because of a technical defect in the information system, the producer of the equipment could be liable (52). At present, there is no EU legislation that directly states the liability of the telemedicine practitioner, although patients can seek compensation when injured as a result of telemedical treatment under the existing laws on medical negligence (61). Two EU Directives, however, do afford consumers some protection in the area of product liability.

Directive 85/374/EEC on product liability establishes the general principle that the producer is liable for damages (19). To establish liability, there must be a defect in the product and harm to the consumer, regardless of whether or not the defect is the result of negligence on the part of the producer. According to Article 2, the definition of product is restricted to movables, so in the health sector, it will be restricted to tangible and technical components that may be defective (52). Furthermore, the Directive gives a broad definition of a producer (Article 3), which can lead to joint and several liabilities of producers (Article 5). When the producer cannot be identified, liability will fall on the supplier (Article 3.3); consequently, a patient injured by a defective telemedical product would have cause for action against the producer, if identifiable, or the medical practitioner. Because medical practitioners are also consumers, they can take action against the supplier or producer if an injury arose through the use of a defective product used in a reasonable and responsible way.

The duties imposed by the Product Liability Directive highlight the importance of stringent product testing, quality control, and risk monitoring (61). According to the Directive, the injured party is required to prove the damage, the defectiveness of the product, and the causal link between the defect and the damage suffered. But in practice, it can be difficult to prove the defectiveness and the causal link.

POLICY IMPLICATIONS AND CONCLUSIONS

Developments in IT have implications for HTA and health systems within the EU. In recent years, the European Commission has adopted a range of legal and nonlegal measures to protect consumers in the information society. Many of the legal measures (directives) indirectly affect health systems in so far as they concern data and database protection, security in electronic transfers, distance selling, electronic commerce, product safety, and liability.

Because few of these legal measures were initiated with health systems in mind, they tend to demonstrate weaknesses and a lack of clarity when applied to health care. This finding reduces their effectiveness in protecting consumers in the health sector. Due to the continuing growth of IT in the health sector and concerns about consumer protection, legal and nonlegal measures need to be further developed at the EU and international level. Where possible, future developments should pay attention to the particular characteristics of health goods and services and health systems.

Greater awareness of legislative matters should inform the process of HTA within the EU and those involved in HTA should be more proactive in monitoring legal developments at EU level and playing a part in informing the legislative process at early stages.

REFERENCES

1. Allaert FA, Barber B. Some systems implications of EU Data Protection Directive. *Eur J Information Systems*. 1998;7:1-4.
2. Altenstetter C. EU and member state medical devices regulation. *Int J Technol Assess Health Care*. 2003;19:228-248.
3. Altenstetter C. Regulation of medical devices in the European Union. In: Baeten R, ed. *The impact of EU law on health care systems*. Brussels: Peter Lang; 2002.
4. Armstrong K, Schwartz JS, Asch DA. Direct sale of Sildenafil (Viagra) to consumers over the Internet. *N Engl J Med*. 1999;341:1389-1392.
5. Arruñada B. *Quality safeguards and regulation of online pharmacies*. Barcelona: Department of Economics and Business; 2001.
6. Ballon IC. *E-commerce and internet law: A primer*. Paper presented at the 2nd Annual Spring Meeting of the State Bar of California, La Jolla, April 27-29, 2001. Available at: www.calbar.org/buslaw/spring2001/ballonpt00.htm. Accessed: July 28, 2003.
7. Banta H, Luce B. *Health care technology and its assessment: An international perspective*. Oxford: Oxford University Press; 1993.
8. Barber B, Treacher A, Louwerse. *Towards security in medical telematics*. Oxford: IOS Press; 1996.
9. Bell J, Gomez R, Hodge P, Mayer-Schönberger. Electronic signature regulation. An early scorecard – Comparing electronic signatures legislation in the US and the European Union. *Comput Law Security Rep*. 2001;17:399-402.
10. Bharvada K. Electronic signatures, biometrics and PKI in the UK. *Int Rev Law ComputTechnol*. 2002;16:265-275.
11. Callens S. Telemededicine and the E-Commerce Directive. *Eur J Health Law*. 2002;9:93-109.
12. Centre de Droit de la Consommation. *Study on the practical application of Directive 92/59/EEC on General Product Safety: Summary of the study conclusions*. Louvain-la-Neuve: Centre de Droit de la Consommation,; 2000.
13. Chalton S. The transposition into UK law of EU Directive 95/46/EC (the Data Protection Directive). *Int Rev Law Comput Technol*. 1997;11:25-32.
14. Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS no: 108. In: *European treaty series*. Strasbourg: Conseil de l'Europe; 1981.
15. Deringer FB. *Product safety and liability in Europe*. In: Freshfields Bruckhaus Deringer; 2002.
16. Desai A. *The European Data Directive and its impact on the export of personal data from Europe to the United States: The Safe Harbour privacy principles*. Available at: http://www.dwt.com/related_links/adv_bulletins/european_ data.htm. Accessed: May 20, 2003..
17. European Commission. *Report from the Commission on the Application of Directive 85/374 on Liability for Defective Products*. Brussels: European Union; 2001 31/01/2001. Report No. COM(2000) 893 final.
18. European Commission. *Convention on the law applicable to contractual obligations (80/934/EEC)*. OJ 1980;L 266(09/10/1980):1-19.
19. European Commission. *Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products*. OJ 1985;L 210(07/08/1985):29.
20. European Commission. *Council Directive 92/59/EEC of 29 June 1992 on general product safety*. OJ 1992;L 228 (11/08/1992):24-32.
21. European Commission. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. OJ 1995;L 281(23/11/1995):31-50.
22. European Commission. *Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases*. OJ 1996;L 077(27/03/1996):20.
23. European Commission. *Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts*. OJ 1997;L 144(04/06/1997):19-28.
24. European Commission. *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector*. OJ 1997;L 024(30/01/1998):1-8.
25. European Commission. *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*. OJ 1999;L 13(19/01/2000):12-20.
26. European Commission. *Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*. OJ 2000;L 178(17/07/2000):1-16.
27. European Commission. *Directive 2001/95/EC of the European parliament and of the Council of 3 December 2001 on general product safety*. OJ 2001;L 11(15/01/2002):4-17.
28. European Commission. *eEurope 2005: An information society for all*. Brussels: European Union; 2002 28/05/2002. Report No.: COM (2002) 263 final.
29. European Commission. *Healthcare*. Available at: http://europa.eu.int/information_society/topics/health/index_en.htm. Accessed: May 20, 2003.
30. European Court of Justice. *Case C-322/01, December 11, 2003*. Deutscher Apothekerverband eV v DocMorris NV and Jacques Waterval. 2003.
31. Eysenbach G. Online Prescribing of Sildanefil (Viagra®) on the World Wide Web. *J Med Internet Res*. 1999;1: online.
32. Eysenbach G, Kohler C, Yihune G, et al. *A framework for improving the quality of health information on the world-wide-web and bettering public (e)health: The MedCERTAIN approach*. MedCERTAIN; 2001.
33. Gibbs D. Harnessing the information society? European Union policy and information and communication technologies. *Eur Urban Regional Studies*. 2001;8:73-84.
34. Hendreson K, Poulter A. The distance selling directive: Points for future revision. *Int Rev Law Comput Technol*. 2002;16:289-300.
35. Hustinx PJ. *Informatietechnologie in de gezondheidszorg*. Utrecht: Verenging voor Gezondheidsrecht; 1999.
36. James S. *What does the EU product safety directive mean for US manufacturers?* Available at: http://www.faegre.com/articles/article_703.asp. Accessed: July 28, 2003.

37. Lipton J. Information wants to be property: Legal commodification of e-commerce assets. *Int Rev Law Comput Technol*. 2002;16:53-66.
38. Long WJ, Pang Quek M. Personal data privacy protection in an age of globalization: The US-EU safe harbor compromise. *J Eur Public Policy*. 200;9:325-344.
39. Makinen MM, Rautava PT, Forsstrom JJ. Restrictions on import of drugs for personal use within the European single market. *Eur J Public Health*. 2002;12:244-248.
40. Muenchinger N, Mekaoui A. Electronic signatures: Regulatory aspects of electronic signatures. *Comput Law Security Rep*. 2002;18:29-30.
41. National Information Center on Health Services Research and Health Care Technology. *Introduction to health care technology assessment-glossary*. Available at: http://www.nlm.nih.gov/nichsr/ta101/ta10108.htm; 2001.
42. Pearce G, Platten N. Promoting the information society: The EU directive on electronic commerce. *Eur Law J*. 2000;6:363-378.
43. PriceWaterhouseCoopers. *HealthCast 2010 E-Health Quarterly. Medical privacy*. New York: PriceWaterhouseCoopers; 2001.
44. Raab CD. Co-producing data protection. *Int Rev Law Comput-Technol*. 1997;11:11-24.
45. Roscam Abbing HDC. Internet, the patient and the right to care for health. *Eur J Health Law*. 2000;7:221-228.
46. Rothchild J. Making the market work: Enhancing consumer sovereignty through the telemarketing sales rule and the distance selling directive. *J Consumer Policy*. 1998;21:279-313.
47. Salaün A. *Consumer protection issues, ESPRIT Project 27028*. European Union: Electronic Commerce Legal Issues Platform; 2000.
48. Smith MF. Data protection, health care, and the new European directive. *BMJ*. 1996;312:197-198.
49. Standing Committee on Copyright and Related Rights. *Protection of databases*. Geneva: Standing Committee on Copyright and Related Rights; 1998.
50. Terry N. MSJAMA: Access vs quality assurance: The e-health conundrum. *JAMA*. 2001;285(:807.
51. Thakur N. *Database protection in the European Union and the United States: The European database directive as an optimum global model*? I.P.Q. 2001;1:100-133.
52. Thematic Working Group 6 of the European Health Telematics Association. *Legal aspects of health telematics*. Brussels: European Health Telematics Association; 2000.
53. U.S. Department of Commerce. *Safe harbor list*. Washington, DC: U.S. Department of Commerce; 2001.
54. U.S. Department of Commerce. *Safe harbor overview*. Washington, DC: U.S. Department of Commerce; 2001.
55. U.S. Department of Commerce. *Safe harbor workbook*. Washington, DC: U.S. Department of Commerce; 2001.
56. U.S. Department of Health and Human Services. *Office for Civil Rights—HIPAA medical privacy—National standards to protect the privacy of personal health information*. Available at: http://www.hhs.gov/ocr/hipaa. Accessed: July 16, 2003.
57. Vajda C, Gahnström A. *EC competition law and the Internet*. European Union: ECIR; 2000.
58. Van Eecke P. Electronic Health Care Services and the E-Commerce Directive. In: Taeymans M, ed. *A decade of research @ the crossroads of law and ICT*. Gent: Larcier; 2001.
59. Walden I. *Anonymising personal data*. Available at: http://research.imshealth.com/IMS%20HEALTH_valueofdata_files/Anonymision%20and%20European%20Data% 20Protection% 20Directive.pdf. Accessed: March 2, 2004.
60. Wilson P. How to find the good and avoid the bad or ugly: A short guide to tools for rating quality of health information on the internet. *BMJ*. 2002;324:598-600.
61. Wilson P. Identifying the European legal and ethical issues of emergent health telematics. In: Thick M, ed. *Taking health telematics into the 21st century*. Abingdon: Radcliffe Medical Press; 2000.