PROTECTING HEALTH CARE DATA: FROM MEDICAL SECRECY TO PERSONAL DATA PROTECTION SOLUTION FOUND?(*)

Roberto Lattanzi Garante per la protezione dei dati personali
Piazza di Monte Citorio, 121 00186 Roma (Italy) r.lattanzi@garanteprivacy.it

1. The Protection of Individuals in the Health Care Sector: From *Habeas Corpus* to *Habeas Data*

The protection afforded by many legal systems has long ceased to only focus on the "concrete" features of the individual [i] as it has also taken account of the dimension that could unquestionably be referred to as the "virtual" one. To the *habeas corpus* – which has been transposed, to a considerable extent, into the informed consent concept – there has been added the *habeas data*; to the consideration of the mainly "physical" features of an individual, there has been added the need to take account of the digital person, i.e. the individual's "electronic body"[ii].
However, both the provisions set out to safeguard "concrete" circumstances and those related to the "virtual" dimension of individuals mirror the transposition into the law of the highest value pursued by all legal systems – namely, respect for human dignity, which is enshrined in Constitutional charters and is actually placed at the beginning of the Charter of fundamental rights of the EU. It is a multifaceted value, and its respect entails taking account of the different social roles played by an individual as well as of his/her concrete situation.
These views have been developing over several years and at different periods in many sectors of the legal system, and have also impacted on the legal framework applying to health care.
Still, it has to be pointed out that the issues related to medical information have long been regarded as minor ones, also by specialised literature. Medical secrecy has gone unchallenged in terms of both ethics and practice, to an even greater extent than in the legal sector – where criminal punishments have been frequently applied. Indeed, the protection of medical data was traditionally committed to medical secrecy, and all exceptions/derogations were left to the lawmaker's discretion – usually in the presence of a public interest considered to override the individual's one (in particular with a view to safeguarding public health), or else on the basis of the patient's consent.

2. Personal Data Protection Legislation As a Means to Overcome the Limitations of Medical Secrecy

In the wake of the massive introduction of information technologies and their cross-sectoral nature, such as to involve all areas of the legal system, personal data protection rules have finally entered the health law arena.
In this manner, data protection legislation has ultimately supplemented the sole protection afforded for a long time to medical information, i.e. professional secrecy. Still, the right to informational self-determination[iii] recognised by data protection legislation is not simply intended for preventing personal information from being disclosed and/or disseminated without justification; in fact, it envisages an "upstream" kind of protection, starting from data collection – and the rules applying to the use of such data. Nor is this right only applicable to certain entities – such as health care professionals; it must be taken into

account by any entity processing medical data, since its rationale consists in the information at issue (here related to health care).[iv] Moreover, data protection legislation is aimed at providing an additional "safeguard" to the data subject – since the processing of medical data must (also) be regulated by the key data protection principles (purpose specification, data minimisation, and data relevance) irrespective of whether the data subject has given his/her consent (which may not always be required).
Apart from the clear-cut recognition of the patient's right to access to his/her data, which has long been denied in many legal systems[v], this is actually the most remarkable qualitative difference compared with the legislation that is only focused on professional secrecy[vi] – which can be overridden by the data subject's consent.[vii]

3. Multi-Function Features of (Medical) Personal Data: So-Called Secondary Uses

It is not to be accepted, however, that the popular (superficial) view prevails whereby the protection of personal data, including medical data, is the response to an unspecified "technological power". In fact, data protection legislation is grounded on the concept that the issue at stake does not consist in unauthorised data intrusions – which here would give rise to violations of medical secrecy; rather, it consists in the ever increasing number of "authorised" accesses to the information (including medical information) based either on the law or the data subject's "consent", for purposes that are increasingly remote from those for which the information had been provided initially.
Medical data tend, by their very nature, to be increasingly disseminated; this was bound to happen, once the conventional dualistic view of the doctor-patient relationship had been overcome. Indeed, this view had already been challenged by the provision of medical treatment via medical teams. The electronic processing of medical data and the attending reduction of costs make it easier to use the data in contexts and for purposes that are different from the initial ones.
Multi-functionality has become nowadays the buzzword in respect of the operation of information systems, just like interoperability; this is why the information in question can be said to move among three main sets.[viii] The first set includes the entities that are directly involved in patient care, i.e. medical and nursing staff. The second set includes the entities working in support of health care activities, mostly in the administrative sector – e.g. dealing with health care payments, or quality controls; in most European countries, these are public entities operating within the framework of national health systems. The third set, which is also the one raising some awkward issues, includes a multifarious gamut of entities that, albeit alien to the medical sector proper, may have a legitimate interest in processing medical data, whereby such interest should be assessed on a case-by-case basis - preferably by lawmakers, even though de facto data protection authorities are often entrusted with this task. The entities in question have been termed social users of health data, or secondary users.[ix] Reference can be made, in this regard, to the use of personal data in order to assess medical activities and reduce health care expenditure[x], plan (and/or implement) social welfare measures, carry out statistical or epidemiological surveys[xi], and more generally perform medical and scientific research[xii] – up to the use of medical information within the framework of insurance or employment contracts, or else in the judicial sector for both criminal and civil proceedings.
The three-tiered system described above, rather than accounting for the considerable reduction of the scope of medical secrecy, actually testifies to the "moving" frontier of the purpose specification principle. The concept initially laid down in the Resolutions by the Council of Europe[xiii], whereby personal data may be processed by strictly complying with

the purpose specification principle, has been replaced by the considerably more flexible principle – which had seeped through the Strasbourg Convention of 1981 (Article 5) and subsequently into EC Directive 95/46 (Article 6) – whereby a data that has been stored for specific, legitimate purposes may be "used in a manner that is not incompatible with such purposes". This is clearly doing away with the main barrier raised against the utilization of a data for purposes other than those for which it had been made available initially.
This crack or, to put it differently, this bridge lowered to allow an interpreter (first and foremost, supervisory authorities) to enter the walled town of data protection can be widened all the more easily insofar as information technology facilitates the processing of the data in question and the demand for such data grows in view of purposes going beyond the individual. Both conditions are currently fulfilled and operate synergically: on the one hand, there is a potentially unlimited capability to store medical information at a low price by means of computerisation; on the other hand, there is the need to reduce health care costs as borne by society.

4. Clinical Records: Between Tradition and Technological Innovation

I think that the issue now cropping up in several legal systems as to whether the medical data contained in a health file (or in clinical records) should be made available online must be put in this context. This is actually a technological application that is bound to be the focus of attention not only of policy- and rule-makers, but also of industry and business entities as well as of the users of complex information systems in the next few years[xiv] – as it might ultimately overcome the (so far) limited storage capabilities of other media, such as microchips. Given the key role this approach is likely to play in the so-called health care management[xv], it is appropriate to consider the relevant issues in greater depth.[xvi]

Suffice it to say here that the (conventional) health file – which is compulsory in many legal systems[xvii] – is intended for gathering the documents kept by each health care body with regard to the respective patients. More specifically, the health file contains, as a rule, a patient's census register data, any consent declarations as rendered with a view to the provision of health care, the outcome of the visits he/she underwent, the relevant diagnoses and prescribed treatments as well as the data concerning specific therapeutic interventions and/or surgical operations.
From being (merely) a prop for the medical practitioner's memory – within the framework of the traditional patient-physician relationship – the health file has turned into a tool to be used by the health staff that, in a given institution, happen to take care of a given patient, in particular on the basis of the "integrated" approach that is a feature of modern hospital care. This growing importance results from the specialisation (and increasing fragmentation) of medical activities as well as, generally speaking, from the depersonalisation of the patient-physician relationship and the public measures adopted in concrete to safeguard the right to health.[xviii] Therefore, the new functions fulfilled by the medical information contained in the health file go well beyond the purposes directly related to the provision of health care.[xix]
Thus, the health file has become one of the main sources of evidence in connection with the appropriate performance of health care activities and has proved accordingly quite helpful in assessing the quality of health care. Additional applications are related to the discharge of administrative tasks that have to do, more or less directly, with the provision of health care – the aim being to achieve increased effectiveness by simultaneously abating costs.[xx] Other objectives might be quoted in addition to those mentioned above, given the

multifunctional approach that is enabled by the electronic processing of information[xxi]; reference can be made – within the framework of the safeguards envisaged by data protection legislation as represented, first and foremost, by data anonymisation – to the lawful processing of medical data in order to get reimbursement for health care activities carried out by third-party payers (whether public or private), or the possible use of such data for the purposes of medical, scientific, epidemiological and/or statistical research.[xxii]

5. Online Health Files: Benefits and Concerns

The arguments supporting the introduction of online health files are well known. Basically, reference is made to cost abatement in processing medical information, from storage[xxiii] to reproduction, information integrity, and the possibility to immediately, "ubiquitously" and fully access the information with allegedly considerable benefits to the patient's health[xxiv] and the overall efficiency of the health care system.[xxv]

However, it would be naïve, to say the least, not to grasp the possible dangers arising to personal values from the technological application now facing us – which is just the latest one in a long series. Indeed, that the discussion is still open – not only within the small circle of data protection academics – was shown by the lively "exchange" between two academics in the medical sector as published on "Le Monde" during the debate that was sparked in France by the *loi relatif à la réforme de l'assurance maladie* – one of the key elements of which is exactly the *dossier médical personnel*.[xxvi]

Whilst it is yet to be established that online health files are bound to become indispensable, as alleged by many commentators, the lawfulness of the processing of personal information in connection with such files will (largely) depend on the approach and the solutions devised with regard to sensitive issues related to the protection of medical data and privacy.[xxvii]

What are the reasons for being cautious? I will now attempt to sketch some of these reasons, taking account, however, that no generalizations are admissible since it is actually necessary to have regard to the concrete configuration of the information systems deployed.[xxviii] The first such reason, which is also the most important one in my view, relates to the inclusion of a person's medical history in a single container – a single, (huge) electronic health file, with the resulting possibility to "massively" access medical information that may not be relevant for the purpose of medical history and/or treatment and therefore should not be available to the physician.[xxix] Indeed, it is no mere chance that the health file may fail to be "closed" only in very limited cases after the patient's release from hospital – usually in order to allow following up a patient affected by certain diseases, as is also the case with so-called "terminal patients".

Consideration should also be given to the discretion that is left to the data subject as to "whether" certain items of medical information – which might actually be relevant – should be disclosed to the medical practitioner. This may be accounted for on different grounds, which are, in part, understandable – such as the intention of seeking additional advice, or personal circumstances that might ultimately prove prejudicial to the data subject.[xxx] In short, it is necessary to carefully consider the alleged impossibility to "break down" medical information, which circulates in bulk because of the supposedly unquestionable efficiency and cost-effectiveness of the measures in question, whilst no account is taken of the close relationship between such information and the most intimate sphere, indeed the very dignity, of an individual.

Some doubts may be raised also in respect of the envisaged possibility for the data subject to freely access the medical information concerning him/her, with the attending cost

abatement for health care institutions – which is fully in line with the provisions currently laid down in data protection legislation and is no longer a matter of discussion[xxxi]. Reference can be made, first and foremost, to the computer "illiteracy" (or "semi-illiteracy") that is a feature of a considerable portion of the population (e.g., the elderly), which would represent a significant hurdle and might ultimately entail the "compulsory" sharing of sensitive data.

Account should also be taken of the consequences (first and foremost, in psychological terms) of allowing access to medical information without the "mediation" of a medical practitioner, given the sometimes dramatic nature of the information at issue.[xxxii] There is a considerable risk of "trivialising" this kind of access as if it were a mere home banking service; to prevent this from happening, appropriate organisational measures should be taken along with the introduction of technological solutions, which must not be – so to speak – "imposed from without".

There are additional issues to be taken into consideration, although no in-depth analysis can be carried out in this paper. In particular, one should not equate all the information possibly fed into a health file (whether medical or not). For instance, the need for different handling and access mechanisms might be related to the specificities of some diseases that carry very strict confidentiality requirements under the law (e.g. in the case of HIV-positivity information[xxxiii]); additionally, the personal circumstances applying to a given patient might impact on the scope of circulation of the information contained in the relevant health file.

Specific measures should be adopted if the medical history to be contained in a health file entails the collection of data related to third parties; this may be the case in psychiatric and psychological cases, or else with regard to genetic data. At all events, it must be possible to keep such data physically or logically separate from those related to the patient. Moreover, one might derive information from the file that is not closely related to the patient's health and has actually to do with other personal circumstances.[xxxiv]

Thus, nothing prevents, in principle, medical information from being computerised and exchanged on a network; it is the manner in which this is to take place that is at issue. Health files, insofar as they are currently envisaged in many legal systems, are kept by each health care professional with regard to individual therapeutic interventions. The rationale seemingly underlying the online health file would appear to consist in creating a single "container" where the medical information on an individual is progressively deposited; such a container is currently kept by the individual health care institution, but it could be "fed" in future with all sorts of information coming from the most diverse health care professionals.

If this were the case, one would not have to do with a mere "technological", i.e. electronic and computerised, version of the conventional health file; in fact, this would entail a qualitative shift compared with the situation envisaged so far by lawmakers and might only be enacted on the basis of a careful law policy analysis to be carried out by the competent decision-makers.

6. Which Data Protection Principles Should also Apply to Online Health Files?

Once again, the validity (and effectivity) of the principles set out in data protection legislation are bound to be challenged by the new processing mechanisms brought about by the online clinical file.[xxxv]

The first – and probably the main – issue has to do with the potentially undifferentiated access to the information contained in the online file[xxxvi]; to avert this danger, reference is usually made to some fundamental data protection principles – first and foremost, data

relevance[xxxvii] and proportionality[xxxviii]. However, application of such principles in complex systems such as those at issue is far from easy, apart from the obvious problems related to security and integrity of the medical information that is stored and transmitted[xxxix], if necessary by means of appropriate encryption mechanisms[xl]. Indeed, a prerequisite for their application is a privacy impact assessment in the project-designing phase, to be carried out by multidisciplinary teams including (at least) physicians, IT experts, and data protection experts, whilst privacy enhancing technologies will have to be deployed in the implementing phase. Both requirements are familiar to data protection scholars, however they encounter remarkable difficulties with a view to being met in practice.
A leading role is bound to be played in this sector by the so-called *Sparsamkeitsprinzip*, whereby information systems should be configured by minimizing the use of personal data so as to rule out their processing if the relevant purposes – with particular regard to the so-called secondary uses – may be achieved in the individual cases either by using anonymous data or via appropriate mechanisms allowing data subjects to be only identified where necessary.

* * *

Thus, online health files will be a veritable benchmark of the continued usefulness of data protection legislation and the supervisory authorities' capability to ensure its effectiveness.
The concerns voiced in the above paragraphs must be taken into account before accepting "blindly" whatever technology has to offer. This holds especially true in the sensitive context of medicine, where bodily health may not be kept separate from the good of the individual as a whole, i.e. as the unity of bodily and spiritual components. In this perspective, the privacy issues addressed so far are one of the elements required to ensure respect for human dignity, which no democratic, constitutional system may allow to be overridden on account of a sort of reckless (albeit likely) "technological inebriation".

---

[*] The opinions contained herein are the Author's own and in no way binding on the Institution where the Author works. The Author would like to thank Mr. Antonio Caselli for translating the text.

[i] As for the ultimate overcoming of the formal concept of individual, regarded merely as the addressee of legal provisions, see L. MENGONI, *La tutela giuridica della vita materiale nelle varie età dell'uomo*, in *Riv. trim. dir. proc. civ.*, 1982, 1117.

[ii] This wording was used by S. RODOTÀ in the *2002 Annual Report by the Italian data protection authority. President's Speech*, Rome, 20 May 2003, p. 7; see also SOLOVE, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 *Minn. L. Rev.* 1137, 1184 *ss.* (2002); *amplius*, SOLOVE, *The Digital Person. Technology and Privacy in the Information Age*, New York – London, 2004, *passim*

[iii] Concerning the *informationelles Selbstbestimmungsrech*t see BVerfG, 15 December 1983, in *BVerfGE*, 65, 1; also in *NJW*, 1984, 419

[iv] It should be added that medical information has ever been considered part and parcel with the most intimate sphere of an individual, a veritable mirror of human dignity – partly because of the possible discrimination resulting from the misuse of such information. Its enhanced protection is grounded on the specific safeguards afforded to sensitive data, which is the category it falls under. See S. SIMITIS, *«Sensitive Daten» - Zur Geschichte und Wirkung einer Fiktion*, *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini*, Bern, 1990, 469; see also R. LATTANZI, *Dati sensibili: una categoria problematica nell'orizzonte europeo*, in *Europa dir. priv*., 1998, 713.

[v] See High Court of Australia, 186 CLR 71, in *Breen v Williams* which confirmed that there is no common law right of access to medical records, and ruled that legislation was required in order to provide the foundations for the said right.

[vi] See, in this regard, ECJ's decision of 20 May 2003, *Rechnungshof* (C-465/00) v. *Österreichischer Rundfunk* and others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v. *Österreichischer Rundfunk* (issued following preliminary ruling requests: *Verfassungsgerichtshof* (C-465/00) and *Oberster Gerichtshof* (C-138/01 and C-139/01) – Austria), in *Raccolta della giurisprudenza* 2003, I-4989, paragraphs 65 and 66.

[vii] Which has proved quite weak as a safeguard, so much so that reference has been made to the "myth of consent" to stress its insufficiency in view of protecting data subjects. See RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, 45; «*autonomy trap*» is the wording used in the same context by SCHWARTZ, *Privacy and Democracy in Cyberspace*, 52 *Vand. L. Rev*. 1609, 1660 (1999).

[viii] See A.F. WESTIN, *Computers, Health Records, and Citizen Rights*, Washington, 1976, 10; the basic conclusions drawn in this study can be also found in the report published more recently by the OFFICE OF TECHNOLOGY ASSESSMENT (OT*A)*, *Protecting Privacy in Computerised Medical Information*, OTA-TCT-576, Washington D.C., UP GPO, 1993, 3.

[ix] This definition has been used extensively. See R.S. MAGNUSSON, *Privacy, Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System*, 24 *Sydney L. Rev.* 5, 8 (2002).

[x] It was exactly for this purpose that the French data protection law was amended in 1999 by decree no. 99-199, which introduced provisions concerning the «t*raitement de données personnelles de santé à des fins d'évaluation ou d'analyse des activités de soins et de prévention*». On the concept of health as a *public good* (whose features consist in *nonrivarly in consumption* and *nonexcludability*) see I. KAUL – I. GRUNBERG – M.A. STERN, *Defining Global Public Goods*, in I. KAUL – I. GRUNBERG – M.A. STERN, *Global Public Good. International Cooperation in the 21st Century*, New York – Oxford, 1999, 2, 3; L.C. CHEN – T.E. EVANS – R.A. CASH, *Health as a Global Public Good*, *ibidem*, 284.

[xi] See the analysis carried out by WESTIN, *Computers, Health Records, and Citizen Rights*, p. 10; similar considerations can be found, despite the time elapsed since Westin's book, in S. KERSTEN, *Datenschutz in der Medizin*, in *CR*, 1989, 1020 as well as in P. SCHWARTZ – J. REIDENBERG, *Data Privacy Law*, 1996, 159. In a decision by the Regional Administrative Court of Latium Region, of 10 July 1989, no. 1009, in Trib. Amm. Reg., 1989, I, 2754, it was ruled that in the regulatory system set up by Act no. 833 of 23 December 1978, with particular regard to Section 58 thereof, "health is considered as the individual's right and the community's interest, which may also fully justify the creation of information tools to be used for epidemiological surveillance; however, such activities must always respect the individual's dignity and freedom, including a patient's right to confidentiality and secrecy with the attending obligation for the health care professional to abide by medical secrecy".

[xii] Reference should be made in this connection to the activities of the EC-funded project "Privacy in Research Ethics and Law" (PRIVIREAL) as reported by D. BEYLEVELD, D. TOWNEND, S. ROUILLÉ-MIRZA and J. WRIGHT (eds.), *Implementation of the Data Protection Directive in Relation to Medical Research in Europe*, 2004; D. BEYLEVELD, D. TOWNEND, S. ROUILLÉ-MIRZA and J. WRIGHT (eds.), *The Data Protection Directive and Medical Research Across Europe*, 2005; D. BEYLEVELD, D. TOWNEND and J. WRIGHT (eds.), *Research Ethics Committees, Data Protection and Medical Research in European Countries*, 2005; D. BEYLEVELD, D. TOWNEND and J. WRIGHT (eds.), *Research Ethics Committees, Data Protection and Medical Research in Europe - Key Issues*, 2006.

[xiii] These are the Resolutions setting out fundamental data protection principles: Resolution (73)22 on the protection of the private life of natural persons with regard to electronic data banks in the private sector, adopted by the Committee of Ministers on 26 September 1973, and Resolution (74)29 on the protection of the private life of natural persons with regard to electronic data banks in the public sector, adopted by the Committee of Ministers on 20 September 1974.

[xiv] Technological innovation in health care has always been the subject of careful analysis; see the study edited by the Commission of European Communities, DG XIII/F AIM, *Data Protection and Confidentiality in Health Informatics. Handling Health Data in Europe in the Future*, Amsterdam (and elsewhere), 1991, *passim*; see also R. WEHRMANN – R. WELLBROCK, *Datenschutzrechtliche Anforderungen an die Datenverarbeitung und Kommunikation im medizinischen Bereich*, in *CR*, 1997, 754. On account of the reasons referred to in this text, long debated projects are likely to be relinquished; this is the case of the smart card-based projects. See, in this connection, T. WEICHERT, *Die elektronische Gesundheitskarte*, in *DuD*, 2004, 391); other technologies such as the online health file would appear to be more promising in this context.

[xv] As regards, in particular, the US legal system, this process started in 1996 after a lengthy debate, when "*The Health Insurance Portability and Accountability Act of 1996*" (HIPPA) was introduced and subsequently passed. This piece of legislation was markedly criticized by the health care industry and was long the focus of attention of US literature. See, for instance, SCHWARTZ, *The Protection of Privacy in Health Care Reform*, 48

Vand. L. Rev. 295 (1995); see also the contributions contained in "*Medical Record Confidentiality and Data Collection*", 25 *J. L. Med. & Ethics* p. 85 (1997).

[xvi] This paper is not considering other technological applications in the health care sector that are more closely related to the provision of health care such as telemedicine; see, in this regard, V. HAZEBROUCQ, *Rapport sur l'état des lieux, en 2003, de la télémédecine française*, Rapport établi, à la demande de Madame la Ministre déléguée à la recherche et aux nouvelles technologies, Paris, 2003, in http://www.ladocumentationfrancaise.fr/BRP/034000522/0000.pdf; in Germany, the *Verordnung über den Schutz vor Schäden durch Röntgenstrahlung* (*Röntgenverordnung* - RöV) of 30 April 2003 introduced the concept of *Teleradiologie*: see W. BERG, *Telemedizin und Datenschutz*, in *Medizinrecht*, 2004, 411. The fundamental need to always ensure data integrity and confidentiality is consistently highlighted: see P.M. ORBUCH, *A Western States' Effort to Address Telemedicine Policy Barriers*, 73 *N. Dakota L. Rev.* 35, 48 (1997).

[xvii] See H. DUCROT, *Le dossier médical informatisé face à la loi française*, in L. DUSSERRE – M. GOLDBERG – R. SALAMON, *Informatique et santé*, Paris, 1996, 87.

[xviii] Its growing use has been also accounted for by the growing amount of litigations related to professional malpractice: see H. FRANZKI – D. FRANZKI, *Waffengleichkeit im Arzthaftungsprozess*, in *NJW*, 1975, 2225, 2226.

[xix] An analysis of the information flows arising inside hospitals can be found in T. BARTA, *Datenschutz im Krankenhaus: Grundzüge der Rechtslage mit Fallbeispielen*, Düsseldorf, 1990, *passim*.

[xx] The use of information technologies for medical data transmission and the resulting data protection issues were addressed by Y. POULLET – R.J. BARCELO, *Health Telematics Networks: Reflections on Legislative and Contractual Models Providing Security Solutions*, typed contribution.

[xxi] See also, with particular regard to medical data, P.M. SCHWARTZ, *Privacy and the Economics of Personal Health Care Information*, 76 *Texas L. Rev.* 2, 15 (1997).

[xxii] On this point, see the groundbreaking essay by H. LILIE, *Ärztliche Dokumentation und Informationsrechte des Patienten. Eine arztrechtliche Studie zum deutschen und amerikanischen Recht*, Frankfurt – Bern, 1980, 15, and the more recent book by A MESCHKE – F.-J. DAHM, *Die Befugnis der Krankenkassen zur Einsichtnahme in Patientenunterlagen*, in *MedR*, 2002, 346.

[xxiii] See F.-J. ORTNER – I. GEIS, *Die elektronische Patientenakte. Rechtsfragen medizinischer Dokumente in digitalen Dokumentationssystemen und digitalen Netzen*, in *MedR*, 1997, 337.

[xxiv] See, for instance, the recent report by M. FIESCHI, *Les données du patient partagées: la culture du partage et de la qualité des informations pour améliorer la qualité des soins*, Paris, 2003.

[xxv] These issues obviously go well beyond national borders; see, regarding Germany, I. GEIS, *DACS – Data Archiving and Communication Services. Zentrale digitale Archivierung von Krankenhausdaten – ein ASP-Konzept*, in *MedR*, 2004, 353.

[xxvi] Reference is made here to the articles by D. LABAYLE, *Le dossier médical informatisé, une nouvelle carte d'identité?* and D. VADROT, *Ne fantasmons pas sur le dossier médical informatisé*, published on 21 and 23 September 2004, respectively.

[xxvii] The need for setting out appropriate regulations was pointed out also in connection with these mainly technological issues. See THE CALDICOTT COMMITTEE, *Report on the review of patient-identifiable information*, London, 1997; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL), *Santé informatique et libertés. Professions libérales de santé*, Paris, 1999.

[xxviii] The considerations made by REIDENBERG J.R., *Information Policy Rules Through Law and Technology*, in Proceedings of the XIX[e] *Conférence internationale des Commissaires à la protection des données*, Bruxelles, 17-19 Septembre 1997, 155, in respect of the pivotal role played by the configuration of the technological infrastructure are fully applicable in this context as well; ID., Lex Informatica: *The Formulation of Information Policy Rules Through Technology*, 76 *Texas L. Rev.* 553 (1998); L. LESSIG, *Code and Other Laws of Cyberspace*, New York, 1999.

[xxix] This risk is bound to be compounded in the near future by the networking of all health care institutions, which would allow retrieving all the information on a given patient, regardless of the places where it is kept, by means of a medical ID code.

[xxx] One might argue that the disclosure of certain items of medical information should be left to the data subject's autonomous decision, or else based on his failure to object to such disclosure; however, apart from any considerations on the manner in which such decisions are taken, one can reasonably question the freedom of the choice made in concrete.

[xxxi] This was the case in the UK, where the *Data Protection Act 1984* was followed by the *Access to Health Record Act 1990* (see J. DAVIES, *Patients' Right of Access to Their Health Records*, in *Medical L. Int'l*, 1996, 189); as for Germany, see LILIE, *Ärztliche Dokumentation und Informationslehre des Patienten*, quoted

above; PETER, *Das Recht auf Einsicht in Krankenunterlagen*, 1989; see also the more recent work by K. NÜSSGENS, *Zur ärztlichen Dokumentationspflicht und zum Recht auf Einsicht in die Krankenunterlagen*, including a description of the historical developments, in C.T. EBENROTH – D. HESSELBERGER – M.E. RINNE (eds.), *Verantwortung und Gestaltung. Festschrift für K. Boujong zum 65. Geburtstag*, München, 1996, 833. It should be pointed out that the possibility for a patient to access the information relating to him/her as contained in the relevant health file has been denied for a long time. See, for instance, X. RIYCKMANS – R. MEERT-VAN DE PUT, *Les droits et les obligations des médecins*, Bruxelles, 1971, 175. On the access to the information contained in the health file, see the comparative study published by the French Senate, LES DOCUMENTS DE TRAVAIL DU SENAT, S*érie legislation comparée, L'information des malades et l'acces au dossier medical*, n. LC 78, Octobre 2000, in <http://www.senat.fr/europe/lc78.pdf>.

[xxxii] This issue was considered in the Italian data protection legislation, which provides that any personal data suitable for disclosing health must be communicated to the data subject (except where the data have been provided by the latter) "exclusively by the agency of a physician to be designated by either the data subject or the data controller" (Section 84(1) of legislative decree no. 196/2003).

[xxxiii] Under Section 5(4) of Italy's Act no. 135/1990, "the results of direct and/or indirect HIV-related diagnostic tests may only be disclosed to the individual undergoing the said tests".

[xxxiv] Reference can be made to the health file concerning a prison inmate, which may only be disclosed to other medical institutions on the basis of appropriate safeguards, or else to the ad-hoc provisions laid down in some legal systems with regard to professional athletes.

[xxxv] However, one should take account in this regard of the actual configuration of online clinical files.

[xxxvi] These considerations are quite similar to those made in the past with regard to the so-called electronic health card, which however can accommodate a significantly smaller amount of information. See, in this regard, COMMISSION OF THE EUROPEAN COMMUNITIES, *Communication from the Commission concerning the introduction of a European health insurance card*, Brussels, 17.02.2003 COM(2003) 73 final, in <http://europa.eu.int/eur-lex/en/com/cnc/2003/com2003_0073en01.pdf>.

[xxxvii] Special measures could be required if the medical history to be included in the health records entails the collection of data concerning third parties – e.g. as regards psychiatric and/or psychological treatments, or the highly sensitive sector of genetic data. There must be the possibility to keep such data separate – either physically or logically – from those concerning the individual patient.

[xxxviii] Some especially sensitive items of information, e.g. those related to HIV and/or AIDS, or genetic data, might have to be left outside electronic health records; another option consists in adopting special measures (e.g. requesting the patient's specific consent) before allowing health care staff to access such information.

[xxxix] The relevant issues have always been taken into account with regard to all technological applications in the health care sector, including the *Entschließung der Datenschutzbeauftragten des Bundes und der Länder* of 9 May 1996, in *19. Jahresbericht des Landesbeauftragten f. den Datenschutz der Freien und Hansestadt Bremen*, 1996, 55. See, in a general perspective, R. ANDERSON (ed.), *Personal Medical Information. Security, Engineering, and Ethics*. Personal Information Workshop – Cambridge, UK, June 21-22, 1996 – Proceedings, Berlin (and elsewhere), 1997, *passim*

[xl] See H. REICHOW – U. HARTLEB – W. SCHMIDT, *Möglichkeiten medizinischer Datenverarbeitung und Datenschutz*, in *MedR*, 1998, 162, 165.