Data protection and confidentiality in healthgrids

WILSON, Petra; Andoulsi, Isabelle; SOLOMONIDES, Tony; BRETON, Vincent; Herveg, Jean

Published in:
Grid-Computing in der Biomedizineschen Forschung, Datenschutz und Datensicherheit

Publication date:
2006

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

1.2. Data Protection and Confidentiality in Healthgrids: The SHARE Project- A Framework for Developing a Roadmap for the Adoption of Grid Technology in Healthcare

P. Wilson[1], I. Andoulsi[2], T. Solomonidès[3], J. Herveg[2], V. Breton[4]

[1] *Internet Business Solution Group, Cisco Systems; Belgium*
[2] *CRID, Namur University; Belgium*
[3] *University of the West of England, Bristol; UK*
[4] *Centre National de Recherche Scientifique, France*

Abstract
The SHARE project [1] on developing a roadmap for the adoption of healthgrids in the European Union focuses one of its work packages on a detailed examination of the legal issues which are relevant to the adoption of grid technologies in the health sector. The project looks at legal issues around data protection, product and service liability and also intellectual property rights.

This chapter focuses on just one of those legal aspects – data protection. Through a detailed examination of the European Data Protection Directive it provides an interpretation of the Directive for the purposes of healthgrids and further outlines the issues which remain to be addressed in national or European level legislation.

Key words
Healthgrid, European, Privacy, Data Protection

1.2.1. Introduction – an outline of the SHARE Project

Most healthcare systems in the developed world are facing multiple challenges in their attempt to maintain an acceptable level of care for their citizens. The principal challenges are often experienced and expressed in economic terms, e.g. as issues of total cost, capacity and responsiveness, and allocation of limited resources. In an attempt to rise to these challenges health systems have increasingly looked to information technology to help, among other things, optimize the distribution and use of resources, to reduce queues and waiting times, to record and so avoid errors, and to provide modern treatments into remote communities.

However, health care systems in Europe have experienced limitations in the application of traditional information networks and technology in healthcare. Governments have naturally focussed on the technical issues that are reasonably well understood, even if solutions are not always easy to obtain: robustness of networks, scalability of systems, readiness to handle a very large volume of data. However, in many respects, these reproduce in the technology some of the problems of the traditional paper-driven systems: inflexibility, maldistribution of resources, failure to understand the needs of medical practitioners, failure to support effective collaboration, and an ultimately simplistic equation of quality with 'choice', while minimal provision is made for just-over-the-horizon future technologies such as genomic medicine and individualized prescribing.

In the face of these challenges, a computational innovation, 'grid' technology, or the grid, has become available to clinicians in the last few years, first as a research tool and then, in the not-too-distant future, as a serious healthcare infrastructure. The grid is not one technology but many, and the use of the singular is somewhat misleading, but it is convenient inasmuch as it echoes 'the internet' to which it is

closely related. Just as the internet, or more precisely the World Wide Web, has provided a massive information platform whose exploitation is limited only by economics (and, in some cases, politics) grid technology promises to scale this up to the provision of unprecedented computational power, online storage and collaboration opportunities. The informatic grid approaches the provision of computational, information and communication services through resource sharing in a seamless and transparent manner, much as the electricity 'grid' provides power to any device plugged into it, irrespective of its purpose or design. Grid computing aims at the provision of a global ICT infrastructure that will enable a coordinated, flexible and secure sharing of diverse resources, including computers, applications, data, storage, networks, and scientific instruments across dynamic and geographically dispersed organizations and communities (sometimes known as 'virtual organizations' or 'VOs'). Grid technologies promise to change the way organizations tackle complex problems by offering unprecedented opportunities for resource sharing and collaboration. Just as the World Wide Web transformed the way we exchange information, the grid concept takes parallel and distributed computing to the next level, providing a unified, resilient, and transparent infrastructure, available on demand, in order to solve increasingly complex problems.

However, the adoption of grids for healthcare is still in its infancy. There are many reasons to this situation. A first obvious reason is that grid technology is still immature and is neither robust nor secure enough to offer the quality of service required for routine clinical use. Another important reason is that all grid infrastructure projects are deployed on national research and education networks which are both separate from the networks used by healthcare structures and **very much less secure** than they need to be. **Another potential obstacle is the legal** framework in the EC member states which has to evolve to allow the transfer of medical data on a European healthgrid. We must also not forget that grids, despite their virtual nature, still require human beings to make choices. Accordingly the economic and benefit case for the use of grids must be made and finally the real work environments and habits of people must be able to accommodate grid based working.

Accordingly the SHARE project has been co-financed by a number of organisations and the European Commission's research and technological development funds in order to develop a roadmap to enhance Grid adoption in the health sector throughout the European Union. The project as a whole looks at a number of issues – in particular at some key use cases in the life science and medical research[2], in this chapter however we look in more detail at the legal and regulatory issues which need to be addressed in order to promote the adoption of grid technology in the European health sector.

Grid technologies, by allowing for more comprehensive and faster creation, monitoring, and update of the medical content of prevention and health promotion schemes, are expected to play an important role in creating more efficient, patient centred systems of healthcare which are able to sustain those core values. It is important therefore that in order to under stand the potential of healthgrids and in order to adopt sensible roadmaps for research on grids and their implementation in the health sector that we understand the key legal issues that are to be addressed.

A common factor amongst many of the connected health tools, whether they use grid technology or more conventional networks, is that they store, process, forward and share data. Some of that data is administrative, some related to objects, such as in radio-frequency identification based tracking of devices, but a great deal of the data is the personal data of patients. Healthcare professionals know they have a duty of confidentiality and a duty of care – they want to exercise both fully in order to provide a safe environment in which patients are treated with due respect for their privacy. The duty to provide care is undoubtedly served by sharing patient records, providing on-line support to colleagues and even giving direct support to patients in their homes via the internet ..... but how does it sit with the co-existing duty of confidentiality?

The purpose of this chapter is to explore the nature of the European response to medical privacy through a detailed examination of the data protection directive. However, data privacy is not the only legal issue which should be addressed in roadmapping healthgrids. It is also vitally important to assess the extent to which product and services liability is adapted to meeting the challenges of healthgrids, as well as considering the wider legal-economic issues such as intellectual property rights. The

SHARE project also looks in some detail at the legal issues arsing from the shared intellectual property of data in healthgrids and of healthgrids themselves. This however is work which will be conducted in the second year of the project and as such is not yet ready to be reported.

1.2.2. European Data Protection

The key principles relevant to the processing of personal data were first established by the Council of Europe [3], and further developed in Directive 95/46/CE of the European Union - the European data Protection Directive [4]. The latter is the major source of legislation, however, the Recommendation made by the Council of Europe is also of importance for the healthcare sector and for the use of grid technology in that sector, since it focuses on the field of medical data and scientific research.

The Directive provides a general framework for the protection of privacy with respect to the processing of personal data in its widest sense. It is important to note here that the Directive is based on the privacy of processing of data, not privacy per se. Thus, the Directive does not confer any special rights of privacy of an individual which might be covered in a Member State's constitution, but rather it provides rules about how personal data may be processed so that the processing itself does not infringe the privacy of an individual. Within the terms of the directive a suitable level of privacy is to be afforded to all data related to a natural person, whether the context of such information is the private, public or professional life of the individual. The Directive thus goes beyond the concept of private life and intimate detail.

The primary purpose of the Directive is to allow the free flow of personal data between the Member States of the European Union, in order to facilitate the establishment and the functioning of the internal market. While its secondary purpose is to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of their personal data. The protection granted by the Directive does, however, go further than the protection of the natural person's intimacy, i.e. generally speaking the protection of each natural person private life. It applies more particularly to any sensitive data relating to natural persons such as data concerning health - including mental health.

To what data does the data protection directive apply?

In deciding if the Directive applies to a particular set of data one must therefore first ask if the data allow the identification of a particular natural person and second if the data are going to be processed by someone (a legal or natural person). The basic principle here is that if a piece of information (a laboratory result) can be linked to a person either by reasonably simple means or even by or with the help of a third party, then the data are considered as identifiable and therefore in the scope of the Directive. It should be noted that this concept is usually construed quite widely. Thus, if the information refers to a group or if it is so complete or so unique as to make it applicable to only a very small number of people (e.g., disease profile, age, gender, postcode, profession all held together) then the data could be classified as identifiable even if no actual identifier were used.

> Given the wide construction it is easy to see that the data contained in a healthgrid, even if not identified by a patient's or study subject's name, will be covered by the terms of article 2(a) of the Directive which state that the term 'personal data' relates to; "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

To whom does the data protection directive it apply?

The data protection rules are addressed primarily to the data controller – this is the legal name of the person who decides the purpose and the means of the processing. This person has the legal duty to ensure that data are handled appropriately in order to ensure the right level of privacy. The data controller is usually a senior staff and whose is officially named as the data controlled by organisation's

governing body. Although the controller is always a natural (real) person, she does not necessarily have to belong to a formally constituted body.

In the case of a healthgrid several doctors or scientists may therefore be separately defined as data controllers - since the data contained in one healthgrid application might have been collected through several different studies or have been extracted from several different patient data sets.

What are the main duties of a data controller?

Any personal data that the controller needs to process for the purposes of his or her professional or other activity must meet certain level of quality. This means that the controller must comply with the Directive's principles concerning data collection and data processing.

First, this means the **data may only be collected for specified, explicit and legitimate purpose.** In practice that will require the controller to define clearly and precisely the purpose(s) for which the data are to be processed. The controller will therefore have to notify the relevant national authority that she is intending to collect personal data and must set out clearly what data will be collected and for what reason. The controller should also be able to explain the purpose and process of the data collection and handling to the data subject.

Second, the **purpose of the processing must be legitimate**. The Directive lists the general conditions under which the processing will be presumed as legitimate and the national legislation further defines what types of data processing are legitimate.

We noted earlier that the overarching purpose of the Directive is to protect privacy within the context of the growth of the internal market. This means that to be legitimate the interests in the data processing must outweigh the interests of the data subject in excluding the processing of the data. Medical data processing is usually legitimate processing because the data subject will have a significant interest in her health data being shared with appropriate professionals if the sharing of the health information will allow better and safer healthcare delivery.

Generally a controller may only process personal data for the purpose which was given when the data were first collected. In some cases the controller may want to re-use the data for another purpose, this will only be legal if the secondary use falls under the uses covered by the national legislation. In many Member States such re-use is permitted if it is for statistical, scientific or historical purpose.
Furthermore, the **data collected should be adequate** for he stated purpose but not excessive. If a researcher collects data in order to carry out a specified research project, she may not collect other data which are not necessary for the study in hand but might be useful at some later date. Once the data are collected, the controller must keep them up-to-date for as long as they are needed for the specified purpose, but should not keep them longer than necessary, and must be rendered anonymous or destroyed the data when the pre-defined purpose of processing has been achieved

If the data are to be processed by a third party – a data processor - this means in practice that the contract between the data controller and the data processor must include a clause that the data processor shall act only on instruction of data controller and that she is also legally responsible in case of any breach of data confidentiality.

The controller also has a duty to ensure that data are stored and processed securely by taking appropriate technical and organisational measures to ensure the security and confidentiality of person identifiable data. According to Article 17 of the Directive, the controller has the obligation to ensure the security of the personal data processed, meaning that he must ensure that the data are not lost, altered, or accidentally destroyed. In order to achieve those two purposes, the controller must implement appropriate technical and organisational measures to protect personal data against, for instance, accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful

forms of processing [5]. In other words, the controller has to construct his system to render it sufficiently secure for the processing of personal data.

This might also imply that in a healthcare setting a structural reorganisation of the hospital or research institute is undertaken to ensure the confidentiality and the security of the data processed. This might include the appointment of a data protection officer in charge of the data protection issues. On the other hand, technical measures could include restricted access to the databases to authorized persons and the utilisation of software protecting the system against viruses or hacking.

Processing **nominative or identifiable** related data in medical research grid would be legitimate if research were given as the purpose of the processing at the time of collection. However, the controller of a healthgrid must ensure that **nominative or identifiable** data are not kept for longer than necessary for the originally defined purpose - in a longitudinal of multi-purpose research study it will therefore usually be necessary to keep the data in an anonymous or pseudonymous form. Furthermore where **nominative or identifiable** data are stored reasonable steps must be taken to hide the true identity of a data subject. Given that the nature of grids is to share the data – often over national boundaries - the steps taken to protect the data must be commensurate with the processing technology. In other words, because a grid is a hi-tech application, state of the art security technology must be used to protect that data stored and processed in the grid.

Are all personal data treated in the same way by the Directive?

A general principle provides that the level of protection offered by the Directive to personal data depends not on the information content, but on the purpose of the data processing. In other words, the potential or actual infringement for the fundamental rights and freedoms of the data subject of privacy and autonomy will be assessed on the basis of the purpose of the processing of personal data.

However, a key indicator remains in the nature of the data. Some data are considered as sensitive and in need of special protection. This is the case of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, as well as data concerning health or sex life and judicial data. For these data the protection depends on the content of the information *and* on the purpose of the data processing. Therefore article 8 of the Directive prohibits the processing medical and other sensitive data.

However, the ban is not absolute. The directive sets out a number of cases in which the collection and processing of medical data may be legitimate. As a result the national legislation of the Member States will allow processing of medical data if:

> The controller has obtained the explicit informed consent of the data subject ; *or*
> If the data are collected to protect the vital interest of the data subject or of another person when the data subject is physically or legally incapable of giving his consent; *or;*
> The data are collected for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services *and* if the data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

The Directive provides the possibility for the Member States to add exemptions for reasons of substantial public interest which could be subject to further specific safeguards, such as the authorisation of the national supervisory authority. Thus, a national transposition of the Directive might allow for the adoption of a national exemption for scientific research or for social security reason.

According to the exemptions to article 8, as listed in its paragraphs and sub paragraphs, a health-grid containing **nominative or identifiable health data** will be legal in terms of data protection only if the **explicit consent** of the data subject was obtained before the data were collected. If this did not happen then the data in the grid a handled by a medical doctor AND the purpose of the grid is the further preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services. If the person handling the data is not a medical doctor but a research scientist he or she will have to be contractually bound in his or her employment contract to maintain the confidentiality of the data. **The only case in which these criteria need not be met is where the Member State in question has passed specific legislation which provides different terms for data collection and processing for the purposes of medical, scientific or historical research**

What rights does the Directive give to the data subject?

The general purpose of the Directive is to facilitate sharing of data in the context of the internal market whilst allowing the data subject to retain appropriate control over the data. Accordingly the Directive requires that data subjects has access to information about the type of data held and the purpose for which it is processed and further the data subject must be allowed to have any errors in the data rectified or, under some conditions, to object to the processing and have it stopped.

A distinction is made between cases where the data are collected directly from the data subject and where they are collected indirectly. If the data are collected directly from the data subject the controller must provide at least identity (name, address, denomination or trade name, etc.) and a description of the purposes of the processing. These purposes have to be specified and explicit, which means that a precise description of the scientific or the statistical project must be given. The processing of sensitive data or medical data normally requires the provision of further information. Guidelines provide, for example, that in case of genetic analysis, the data subject should be informed about the objectives of the analysis and about the possibility of unexpected findings [6].

When personal data have not been obtained directly from the data subject, the controller should, before considering the way of processing these personal data or the right time to inform the data subject, assess whether they comply with the requirements for re-use of data [7].

Moreover, the duty of information does not apply when data are indirectly collected for processing for statistical purposes or for the purposes of historical or scientific research, if the provision of such information is impossible or would involve a disproportionate effort.

All data subjects have the right to request specific information about their own personal data that are processed by the controller. Moreover, where medical data are processed, data subjects may ask a healthcare professional to exercise their access right. Upon request, the controller will then have to provide the data subjects with information such as whether or data processing data relating to them is taking place. He will also have to inform them about the purpose of the processing, the categories of data and the data being processed, the recipients or categories of recipients to whom the data are disclosed and the source of the data. However, the Directive allows Member States to exempt the controller from respecting the data subject's access right where the purpose of the processing is scientific research, or when data are kept in personal form for a period which does not exceed the period necessary to create statistics. The Directive, however, subjects the granting of that exemption to the condition that there is clearly no risk of breach of the data subject's privacy. Moreover, data may not be used in order to take measures or decisions regarding any particular individual.

Under the Directive, a data subject has the right to ask for data to be corrected, erased or blocked where their processing does not comply with the provisions of the Directive [8]. This is particularly the case where personal data are incomplete or inaccurate. This right means that the controller must correct, erase or block the data as required by the data subject, in a reasonable period. Blocked data cannot further be processed, used, or communicated without the data subject's consent. In addition, if the controller has disclosed the data to third parties, he has to notify them about any correction, erasure

or blocking carried out. This notification of correction, erasure or blocking of data does not have to be performed if it proves to be impossible or involves a disproportionate effort [9].

The Directive allows Member States to exempt the controller from the obligation to respect the data subject's right of correction in case of processing for purposes of scientific research, or when data are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics[10]. Furthermore the Directive provides that the data subject has the right to object to the processing of his data. When there is a legitimate objection to the data processing, the controller may no longer process the concerned data or communicate them to recipients, and must ensure they are erased [11].

The controller of a healthgrid must therefore first ensure that he knows from whom the data is being collected, because if it is being collected from the data subject directly from a data subject he must inform the data subject about the purpose of the collection. This may be implicit information if the controller is the data subjects treating doctor, but in the case of a scientist collecting data for research purposed directly from the data subject the purpose should be explicitly stated. If the data are being drawn from existing records the data subject should be informed about the research if it is not unduly difficult or costly to do so. Next he must ensure that he can grant access to the data to the data subject if the data subject requests it, unless national legislation provides that this is not necessary. If any of the provisions safeguarding the data subject's interests are not complied with, the data subject would have the right to demand that his or her data are withdrawn from a study or database. It is therefore very much in the scientist's interests to ensure he complies with the legislation because not only might national legislation levy a fine for non-compliance a data subject could severely disrupt a study if he discovered that data were unlawfully held and exercised his right to have them erased. The scientist should also ensure that the data collected are accurate, because if they are not the data subject will have a right to demand they are corrected and if this is not possible that they are erased.

What are the implications for Cross-Border Data Sharing?

Healthgrids provide doctors, researchers and health system planners the opportunity to support areas of healthcare such as medical imaging and image processing; modelling the human body for therapy planning; pharmaceutical research and development; epidemiological studies; and genomic research and treatment development. However, in order to be truly effective such grid applications must to draw together huge amounts of data from disparately located computers - which of course implies data sharing across jurisdictions and the sharing of responsibilities by a range of different data controllers.

National legislations of the different EU Member States should be harmonised by now, and the transfers of personal data between these Member States should not create any problem. Thus , a data controller established on the territory of one Member State should not fear by transferring the data he processed to another controller established in another Member State, that these data would not be correctly protected as the second Member State does not provide for the same level of protection of personal data as the first one.

This would be the case if all Member States had transposed the Directive in the same way. But differences are already to be found in the member States' legislations as regards the definitions of key concepts of the Directive such as 'personal data', 'processing' or 'controller'. Moreover, the Directive itself allows the Member States to *"adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitute a necessary measure to safeguard:*

(a) national security;
(b) defence;
(c) public security;
[...]".

There might thus be differences in the level of protection granted to personal data between the EU Member States, which might be a problem for the implementation of the Healthgrid technology on the whole territory of the European Union. However, it is important to note that even if there are differences in the levels of protection of personal data between the Member States, these differences are of minor importance, as the implementation of the Directive already ensures a high level of protection for personal data. These differences in the levels of protection of personal data between the Member States can not even constitute barriers to data transfers as Article 1, paragraph 2 of the Directive prescribes:

"Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1 (i.e. the protection of data subjects' fundamental rights and freedoms)".

This is not always the case as what regards the transfer of personal data towards other countries located outside the European Union and the European Economic Area (EEA) which governed by specific conditions [12] that need to be met in addition to the requirements for the communication of personal data to third parties as analysed above.

The general rule is that the controller should refrain from transferring personal data to a recipient located in non-EEA countries. However, the Directive provides that if the data subject his consent unambiguously to the proposed transfer; or the transfer is necessary for the performance of a contract between the data subject and the controller (as might be the case for healthcare) or if the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party (as might be the case in medical research undertaken for aspefic patient or group of patients or the transfer is necessary in order to protect the vital interests of the data subject.

Moreover, the Directive states that Member States may authorise a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of protection of personal data, where the controller adduces adequate safeguards through appropriate contractual clauses between the sender and the recipient of the personal data. In this frame, the European Commission proposes standard contractual clauses that ensure an adequate level of protection of transferred personal data.

However, European Directive does not set specific conditions for the transfer of **medical** data to non EU (and non EEA) countries, but the Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the protection of medical data, adopted on 13 February 1997, does so. It establishes additional rules for the transfer of medical data to a country which does not have an equivalent level of protection of medical data as the one granted on the territory of the European Union.

Furthermore, some countries, such as Argentina, Isle of Man, Guernsey and Switzerland, have been recognised by the European Commission as ensuring an adequate level of protection. This means that the European Commission has decided that these countries have a level of protection of personal data in some way equivalent to the one available in the Member States of the European Union. The transfer of data to companies or other legal entities located on the territory of the United States which adhere to the US Department of Commerce's Safe Harbour Privacy Principles is also allowed. The European Commission moreover allows the transfer of personal data to recipients located on the territory of Canada, provided that these recipients are subject to the Canadian Personal Information Protection and Electronic Documents Act (also called the 'PIPED Act').

1.2.3. Conclusion

From the discussion of the basic concepts and duties of the data Protection Directive and its impact on healthgrids shows that when healthgrids are used for treating patients or planning care the requirements to of the legislation provide that so long as the data subject has consented or the data collected and processed by medical professionals the balance of rights weighs in favour of data collection - that

is, it is assumed that the patient's general interest in obtaining treatment or advancing medical care outweighs his interests in privacy.

However, most of the newly developed health gird applications which exist and are currently running are for longer term purposes – that is research, preventative medicine or healthcare planning and are not controlled by medical professionals but by research scientists. Where this the case Member States have the possibility to the enact specific legislation covering specific tools such as healthgrids in order to exempt the scientist using running healthgrids from some of the more onerous duties of the Directive. Member States could, for example adopt specific legislation to encourage the linking of diagnosis specific databases across a region or state in order to support research into a given disease - however to no Member States have specifically addressed legislation to this particular issue and so healthgrids drawing the data and data processing power of many hospitals tighter are burdened with heavy data protection requirements which could deter scientists from using adopting health gird technology and using its enhanced computational and data acquisition power.

Perhaps more significantly little attention has been paid to the specific needs of data sharing for healthgrids across European borders and outside the Union. If healthgrids are really to grow to their full potential and deliver their promise adjustments must be made to national and supranational legislations to re-assure would-be healthgrid users that it is legal to share health related data using grid technology. This in turn implies the development and adoption of robust guidelines developed specifically for the healthgrid context which address the balancing of interests between an individual's privacy and medical advancement.

References

1. Project Number FP6-2005-IST-027694 Co-Funded Under The Information Society Programme Of The European Commission
2. 2. Details of the full consortium as well as the public deliverable of the project may be found at www:
3. Convention No. 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted on 28 January 1997; Recommendation No. R (97) 18 of Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes, adopted on 30 September 1997.
4. Directive 95/46/CE 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 free movement of such data, OJ L 281, of 23 November 1995, 31-50.
5. Directive 95/46/CE, art. 17, 1, § 1.
6. See Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the protection of medical data adopted on 13 February 1997.
7. See paragraph 2.2. supra.
8. Directive 95/46/CE, art. 12(b).
9. Directive 95/46/CE, art. 12 (c).
10. Directive 95/46/CE, art. 13, 2.
11. Further to this the Council of Europe has recommended in Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics, that where processing is conducted for scientific or statistical reasons, the data subject may withdraw his collaboration. This is however not binding upon Member States, but is considered as good research practice.
12. Directive 95/46/CE, articles 25 and 26.