

## RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

### The ban on processing medical data in european law

Herveg, Jean

*Published in:*  
Challenges and Opportunities of HealthGrids

*Publication date:*  
2006

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

#### [Link to publication](#)

*Citation for pulished version (HARVARD):*

Herveg, J 2006, The ban on processing medical data in european law: consent and alternative solutions to legitimate the processing of medical data in healthgrid. in *Challenges and Opportunities of HealthGrids: Proceedings of Healthgrid 2006*. Studies in Health Technology and Informatics, no. 120, IOS Press, Amsterdam, pp. 107-116.

#### **General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

#### **Take down policy**

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.



**From the SelectedWorks of Jean HERVEG**

---

January 2006

The ban on processing medical data in European Law : consent and alternative solutions to legitimate the processing of medical data in healthgrid

Contact  
Author

Start Your Own  
SelectedWorks

Notify Me  
of New Work

---

Available at: [http://works.bepress.com/jean\\_herveg/8](http://works.bepress.com/jean_herveg/8)

# The Ban on Processing Medical Data in European Law : Consent and Alternative Solutions to Legitimate Processing of Medical Data in HealthGrid

Jean Herveg

*Maître de conférences aux FUNDP – Faculté de Droit – D.E.S. D.G.T.I.C.  
Centre de Recherches Informatique et Droit  
Avocat au barreau de Bruxelles*

**Abstract.** 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 bans the processing of medical data owing to their highly sensitive nature. Fortunately the Directive provides that this ban does not apply in seven cases. The paper aims first to explain the reasons for this ban. Then it describes the conditions under which medical data may be processed under European Law. The paper investigates notably the strengths and weaknesses of the data subject's consent as base of legitimacy for the processing of medical data. It also considers the six other alternatives to legitimate the processing of medical data.

**Keywords.** Processing of Medical Data – Legitimacy – European Law – HealthGRID

## INTRODUCTION

1. 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 [1] bans the processing of personal data concerning health (medical data) [2]. Naturally this prohibition applies equally to the processing of medical data in HealthGrid. This *petitio principii* could have led to serious problems, notably for HealthGrid, if the Directive had not provided that this ban does not apply in several cases [3]. Before considering these exceptions, it seems relevant to remind the reason for this ban particularly since the latter apparently opposes the free movement of personal data [4].

### 1. THE BAN ON PROCESSING MEDICAL DATA

2. The regulation of the processing of personal data is based upon two main ideas. The first idea is that the economical, social, cultural and individual activities, with no public or private distinction, require in various extents the processing of information

relative to natural persons. The second idea, intimately bound to the first one, is that natural persons must be protected against any infringement to their fundamental rights and freedoms that might arise from the processing of information relative to them. In other words, the processing of personal data is frequently needed for multiple good reasons. But, in the same time, the processing of personal data induces the danger to expose natural persons to grave risks of discriminations or infringements to their fundamental rights and freedoms. With respect to this and with this aim in view, the processing of personal data must comply with several rules expressing the balance between all the interests in presence. In this context Directive 95/46/EC aims to ensure the protection of fundamental rights and freedoms of natural persons (data subject), and in particular their right to privacy with respect to the processing of personal data [5]. This protection requires regulating the processing of personal data in order to prevent any infringement to the fundamental rights and freedoms of the data subject.

To be effective and coherent this regulation has to be built on the analysis of the risks capable to affect the fundamental rights and freedoms of the data subject. It is only possible to determine the conditions under which personal data can be processed in full respect of the fundamental rights and freedoms of data subjects when these risks are identified.

This risk assessment is particularly important since the recent evolutions of Information and Communication Technologies have multiplied the possibilities to process personal data and therefore increased the risks of infringement to the fundamental rights and freedoms of the data subject.

The use of a new technology such as HealthGrid should naturally induce the assessment of the new risks attached to its implementation especially in healthcare regarding the protection of medical data.

3. The general principle is that the risk of infringement to the rights and freedoms of the data subject does not depend on the information content. But the risk depends on the purpose of the processing of personal data. In other words the potential or actual danger for the fundamental rights and freedoms of the data subject has to be assessed regarding the purpose of the processing of personal data.

But the principle is slightly – though not entirely – different for sensitive data [6]. It is commonly admitted that the sole content of these data already exposes the data subject to the risk of infringement of his or her fundamental rights and freedoms, whatever could be the purpose of the data processing. Put differently, any use of sensitive data is susceptible to create grave risks of discrimination for the data subject. Therefore sensitive data require a special protection taking into account their content and the purpose of their processing.

With this end in view the Directive has decided that “*data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed (...)*” [7]. The ban on processing medical data is the special protection provided by the Directive to ensure the respect of the fundamental rights and freedoms of the data subject regarding the processing of his or her medical data.

Hence the ban on processing medical data should not be seen as opposed to the free movement of personal data. The ban on processing medical data is more a limit than an exception to the free movement of personal data. In fact the free movement of personal

data can only be conceived in the full respect of the fundamental rights and freedoms of the data subject and this respect includes the ban on processing medical data.

## **2. EXCEPTIONS TO THE BAN ON PROCESSING MEDICAL DATA**

4. Nevertheless the Directive grants permission to process medical data in seven hypotheses. In these ones the legitimacy of the processing of medical data (the balance between the interests in presence [8]) is formally presumed (cf. *infra* the necessity to really assess its legitimacy). This comes from the fact that, in principle, the situations described in these hypotheses should justify the processing of medical data, without prejudice for the other conditions ensuring the lawfulness of the data processing.

These exceptions to the ban on processing medical data must be restrictively interpreted.

The processing of medical data is strictly forbidden beyond these exceptions.

The first hypothesis granting permission to process medical data is the consent of the data subject. The data subject's consent is frequently presented as the natural base for the legitimacy of the processing of medical data.

### *2.1. The consent of the data subject*

5. According to the Directive the ban on processing medical data does not apply where the data subject has given his or her explicit consent to the processing of his or her medical data [9].

In this case the Directive entrusts the data subject with the power to authorize the processing of his or her medical data [7]. This empowerment of the data subject represents without any doubt a very strong expression of his or her informational self determination – the power of the data subject upon his or her personal data – [10].

But this empowerment could also surprise. Is the data subject always capable to decide in a reasonable way about the processing of his or her medical data? Isn't it too dangerous to give the data subject such power when most of the time he or she represents the "weakest" party or at least the "demanding" person in the processing his or her medical data? By example, how could a patient oppose the processing of his or her medical data for scientific purpose (ex. for a clinical trial) before a surgery or any other investigation? How to ensure the validity of the data subject's consent and avoid a complete masquerade?

This empowerment of the data subject should not be seen as unlimited or under no control. In fact when given this power the data subject has to evaluate the interest(s) that could justify the processing of his or her medical data. With this end in view the data subject has to put correctly into balance the interests in presence and to act accordingly. Otherwise the consent will not be able to legitimate the processing of his or her medical data (see *infra* about the real control of the legitimacy of the processing of medical data and the determination of the interests in presence).

The Directive confirms this analysis.

6. Regarding the Directive the data subject's consent means “*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*” [11].

First the consent has to be indubitable, indisputable, without any doubt.

Then the consent of the data subject must have been freely given. In this regard the consent has to be free of any vice, constraint or pressure. With respect to this any direct profit (such as the benefit for his or her health) or indirect profit (such as the participation to the progress of medical science) for the patient should not affect automatically the validity of the data subject's consent. Would the financial retribution of the data subject (beyond the cover of his or her eventual expenses) invalidate his or her consent? Again, the answer to this question should not be absolute. It should depend upon the circumstances of each considered case and on how the applicable law deals with the protection of the data subject.

Moreover the consent of the data subject has to be specific and informed. To be specific reminds insistently that the data subject must know exactly what he or she consents to. The latter implies necessarily the prior and adequate information of the data subject concerning the processing of his or her medical data. Without this prior and adequate information the consent of the data subject shall not be specific. Therefore and in any case the consent of the data subject could not ground the processing of his or her medical data.

In this view the next question is logically the determination of the detail level of the provided information to the data subject. Articles 10 and 11 of the Directive determine the minimum content of this information. The latter must permit the complete enforcement of all the aspects of the data processing – such as the data quality, the data subject's rights, the security and confidentiality measures, the notification to the supervisory authority, etc. –. However there is no doubt that the information has to be more accurate and complete particularly since very sensitive data as medical data are processed.

In any case the data subject may not give an unspecified or uninformed consent to the processing of his or her medical data.

Further processing of medical data is prohibited when incompatible with the initial purpose for which data have been collected.

The consent must be given prior the time of the data collection. It must not be given necessarily at the same time; it only has to be obtained prior the processing.

7. The consent of the data subject must be explicit to allow the processing of his or her medical data [12].

*A contrario*, the requirement of an explicit consent should exclude any implicit consent – whatever could mean this last notion –. With respect to this, beyond the indisputable character of the data subject's consent, its explicit characteristic presumes that it has been expressed. Several Member States have decided to transpose this requirement by asking for a written consent from the data subject.

However the explicit consent could be deduced from some other behaviour of the data subject especially regarding the circumstances of the case. Indeed some positive actions could express the explicit consent of the data subject to the processing of his or her

medical data, such as the participation to a foundation fighting against the disease affecting the data subject or as the demand to be treated in a special medical unit notoriously known as being a research unit.

8. In all these circumstances the consent of the data subject induces a presumption of legitimacy of the processing of his or her medical data. It is assumed that the data subject has correctly assessed the interests in presence and acted accordingly. If the data subject has not correctly assessed the interests in presence and if the interests in presence are not respected, his or her consent will not legitimate the processing of his or her medical data. The latter will not be legitimate on this ground.

In other words the consent of the data subject does not exonerate the data controller from pursuing a legitimate purpose (inducing the balance between the interests in presence) and the consent of the data subject may not cover the illegitimate interest or the lack of interest of the data processing.

9. The Directive provides that Member States may oppose the possibility for the sole consent of the data subject to lift the prohibition from processing medical data [13].

10. In any case the data subject may always revoke his or her consent to the processing of his or her medical data. What are the consequences of this revocation? Does it mean that, in the future, new operations upon the data subject's medical data will not be any more possible (without any effect on the existing data processing) or do we have to consider that the operations realised upon the medical data on the ground of the initial consent of the data subject may not be pursued ?

Since the data subject has revoked his or her initial consent there is no more legitimate base for the processing of the medical data. The operations may not be pursued. That does not mean that the past operations realised upon the medical data of the data subject are now unlawful. It simply means that they can not be pursued except on the ground of another base of legitimacy.

11. Finally the Directive gives no formal indication on the nature of the consent given by the data subject or on the possible contractual relationship between the data controller and the data subject.

In our views the solution to these questions depends on how the applicable law deals with the relationship between the data controller and the data subject and with the relationship between the data subject and his or her personal data. In any case the possible contract should obey the special rules imposed through the transposition of the Directive in the applicable law such as the characteristics of the data subject's consent, the data quality, the data subject's rights, the security and confidentiality measures, the notification to the supervisory authority, etc.

The applicable law determines also the capacity to consent for underage or disable persons.

Regarding the previous developments, it is not sure that the consent of the data subject represents the best solution to ground the legitimacy of the processing of medical data in HealthGrid. Fortunately the Directive provides alternative solutions to legitimate the processing of medical data.

## *2.2. Carrying out obligations and specific rights of the data controller in the field of employment law*

12. The ban on processing medical data does not apply where the *“processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards”* [14].

With respect to this, the purpose of the data processing is only to allow the data controller to fulfill his obligations and rights in the matter of Employment Law, the latter must be specific. This hypothesis seems to cover Medical Inspection.

Then the processing of medical data has to be necessary and not only useful to this purpose. Therefore the data controller has to prove the necessity to process medical data to carry out his obligations and specific rights in the field of Employment Law.

Finally this kind of processing has to be authorized by the applicable law providing for adequate safeguards, the latter being not further determined.

## *2.3. Vital interests*

13. The third hypothesis allowing for the processing of medical data is where *“processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent”* [15].

The notion of *“vital interest”* means expressly and exclusively the situation of an imminent danger to the life of a natural person. This covers the protection of the vital interests of the data subject but also of any other natural person. However in this last situation the Directive adds that the data subject must be physically or legally incapable of consenting to the processing of his or her medical data. It can not be deduced from this disposition that the data subject, physically or legally capable of consenting, could, without any consequence, refuse to authorize the processing of his or her medical data when the vital interests of another person are at stake. The qualification of this behaviour should be qualified under the applicable law.

## *2.4. Non profit organisation*

14. The processing of medical data could be legitimate where the *“processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects”* [16].

With respect to this the organization must have a non profit purpose and the latter has to be relative to the exercise of fundamental rights and freedoms [7].

### 2.5. *Data manifestly made public and establishment, exercise or defence of legal claims*

15. The ban on processing medical data does not apply where “*the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims*” [17].

It has to be reminded that, even if manifestly made public by the data subject, the processing of his or her sensitive personal data falls nevertheless under the scope of the Directive. Hence the data controller must comply with all the other conditions ensuring the lawfulness of the data processing.

### 2.6. *Healthcare purpose*

16. The ban on processing medical data does not apply “*where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy*” [18].

The healthcare purpose should be interpreted broadly [19] including the management of healthcare services. The latter should include secondary purposes necessary to provide healthcare such as medical secretaries, computer Departments, etc. By contrast, this hypothesis does not include Social Security purposes or Public Health purposes (cf. *infra* 2.7).

Medical data must be processed by a health professional, but this last notion has not been further defined. The health professional has to be subject under national law or rules established by national competent bodies to professional secrecy.

When not processed by a health professional, the processing may be carried out by another person if he or she is subject to an equivalent obligation of secrecy notably due to his or her status or by way of contractual stipulation or term.

It is quite remarkable that the patient’s consent is not required to legitimate the processing of medical data. Might there be confusion with the consent to the provision of healthcare ?

### 2.7. *Reasons of substantial public interest*

17. The Directive grants Member States with permission to lay down additional exemptions for reasons of substantial public interest [20]. Hence the Member State has to prove in each case the real existence of the considered substantial public interest(s).

The Directive had essentially in mind substantial public interests relative to Public Health and Social Security “*especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system (...)*” [21]. It had also in mind scientific research and public statistics [21].

The cases where medical data may be processed must be laid down by national law or by decision of the supervisory authority.

But Member States may only allow for the processing of medical data if these exceptions are subject to the provision of suitable safeguards to protect the fundamental rights and freedoms of the data subjects and especially their right to respect for private life [21]. The Directive does not determine these safeguards.

Member States must notify to the European Commission the exemptions to the ban on processing medical data adopted on this base [22].

Member States must determine the conditions under which a national identification number or any other identifier of general application may be processed [23].

### **3. REAL ASSESSMENT OF THE LEGITIMACY OF THE PROCESSING OF MEDICAL DATA**

18. The legitimacy of the processing of medical data is not complete when only formally fitting into one of these exceptions to the ban on processing medical data, even with the consent of the data subject. Indeed these exceptions are only hypotheses where the legitimacy of the data processing is formally assumed.

Now the legitimacy of the processing of medical data – the balance of the interests in presence – has to be really assessed.

First the interests in presence have to be identified. Are they only the interests of the data controller and of the data subject or should we also consider the interests of third concerned parties and of the whole society? In our view these two last categories of interests should be taken into account when evaluating the legitimacy of the processing of medical data.

Then the explicit and valid consent of the data subject presumes, until contrary proof, the existence of an acceptable balance between the interests in presence in the processing of his or her medical data. However, in this case, it is quite difficult to assume that the data subject has adequately taken into account interests other than one's own.

In any case the processing of medical data will not be legitimate if the balance between the interests in presence is not respected, even with the regular consent of the data subject.

19. But the legitimacy of the processing of medical data is definitely and very usefully strengthened by the additional consent of the data subject. That is the reason why we must firmly approve and recommend the ethical practice aiming to obtain the consent of the data subject when processing medical data. This practice is frequent in the conduct of clinical trials and in telematic networks in healthcare.

20. Finally, it has to be stressed that the data controller may not legitimate the processing of medical data on other bases. That excludes necessarily the use of the hypotheses of formal legitimacy enumerated in article 7 of the Directive for non-sensitive personal data. By example the data controller may not legitimate the

processing of medical data by the balance of the interests in presence without respecting the hypotheses enumerated in article 8.

## CONCLUSIONS

21. The protection of medical data implies to fix the rules applicable to the processing of medical data and hence to determine their conditions. With regard to their highly sensitive nature, medical data require a special protection taking into account their content and the purpose of their processing. Therefore Directive 95/46/EC has decided to prohibit the processing of medical data. However the Directive provides that this ban does not apply in several cases. In these cases the legitimacy of the processing of medical data is formally assumed without prejudice for the other conditions ensuring the lawfulness of the data processing. These exceptions to the ban on processing medical data have to be restrictively interpreted.

The explicit and valid consent of the data subject constitutes the very first source of legitimacy for the processing of his or her medical data even if, at the same time, it is the weakest base to legitimate the processing of medical data due to the strict conditions for its validity and to the possibility for the data subject to revoke his or her consent at any time and without justification (but with reasonable notice in some case?).

Nevertheless even if the data controller may legitimate the processing of medical and even with the consent of the data subject, the legitimacy of the data processing must be really assessed in each case by the balance of the interests in presence. These include the interests of the data subject, of the data controller, of third concerned parties and of the society.

In any case the consent of the data subject does not cover the lack of legitimacy or the illegitimacy of the processing of his or her medical data. The consent of the data subject only creates the presumption of legitimacy of the processing of medical data until proof of the contrary.

Finally we must approve and recommend very strongly and warmly the ethical practice requiring the consent of the data subject when processing medical data, even the latter might rely on another base of legitimacy.

## Endnotes

- [1] On the Directive : Y. Poullet, M.-H. Boulanger, C. de Terwangne, Th. Leonard, S. Louveaux et D. Moreau, La protection des données à caractère personnel en droit communautaire, *Journal des Tribunaux de droit européen*, Bruxelles, Ed. Larcier, 1997, p. 121 (in three parts).
- [2] *Directive 95/46/EC*, art. 8.1. The notion of medical data includes all information relative to any aspect, physical or psychological, of the present, past or future health condition, good or bad, of a living or dead natural person. On the definition of medical data : *Explanatory report of Convention n° 108*, recital 45 ; *Rec. (97) 5 of the Council of Europe relative to the protection of medical data*, art. I of the annex ; *C.J.C.E.*, 6 Nov. 2003, Bodil Lindqvist, case C-101/01, obs. C. de TERWANGNE, « Affaire Lindqvist ou quand la Cour de justice des Communautés européennes prend position en matière de protection des données personnelles », *R.D.T.I.*, 2004, pp. 67-99 ; *Groupe européen d'éthique des sciences et des nouvelles technologies*, avis n° 13 du 30 juillet 1999 sur les aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information.
- [3] *Directive 95/46/EC*, art. 8.2.

- [4] On the free movement of personal data : *Directive 95/46/CE*, art. 1.2, and recitals 3, 4, 5, 6, 7, 8, and 9.
- [5] *Directive 95/46/CE*, art. 1.1.
- [6] Usually, sensitive data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and personal data concerning health or sex life.
- [7] *Directive 95/46/CE*, recital 33.
- [8] Cf. *infra* for the identification of these interests.
- [9] *Directive 95/46/CE*, art. 8.2. a. The national law may provide that the data subject's consent may not lift the prohibition.
- [10] On the notion of informational self-determination : Fr. RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Paris, Bruylant, L.G.D.J., 1990, p. 588-589, n° 532 : « (...) *La juridiction constitutionnelle a déduit du droit de la personnalité l'un de ses attributs, à savoir : « le pouvoir reconnu à l'individu et résultant de la notion d'auto-détermination, de décider en premier lieu lui-même quand et dans quelle mesure des faits relatifs à sa propre existence sont divulgués (...) Cet attribut du droit de la personnalité est appelé « droit à la maîtrise des données personnelles » (...) Il n'est toutefois pas sans limite. (...) »* ; Council of Europe, *Resolution 1165* (1998), 26 June 1998, Droit au respect de la vie privée (24th Session), point 5.
- [11] *Directive 95/46/CE*, art. 2, h.
- [12] *Directive 95/46/EC*, art. 8.2, a) and recital 33.
- [13] *Directive 95/46/EC*, art. 8.2, a).
- [14] *Directive 95/46/EC*, art. 8.2, b).
- [15] *Directive 95/46/EC*, art. 8.2, c).
- [16] *Directive 95/46/EC*, art. 8.2, d).
- [17] *Directive 95/46/EC*, art. 8.2, e).
- [18] *Directive 95/46/EC*, art. 8.3.
- [19] However the Directive seems to include only certain purposes relative to healthcare (cf. recital 33).
- [20] *Directive 95/46/EC*, art. 8.4.
- [21] *Directive 95/46/EC*, recital 34.
- [22] *Directive 95/46/EC*, art. 8.6.
- [23] *Directive 95/46/EC*, art. 8.7.