BRILL

EUROPEAN JOURNAL OF HEALTH LAW 21 (2014) 260-270

European Journal of Health Law

brill.com/ejhl

# Data Protection and the Patient's Right to Safety

*Jean Herveg* *
Faculty of Law, University of Namur, Belgium

## Abstract

The article investigates the issue of knowing whether or not the proposal for a general data protection regulation could improve the patient's safety. This has been analyzed through the four main contributions that should be expected at least from data protection to the patient's safety. In our view, data protection should help supporting efficient information systems in healthcare, increasing data quality, strengthening the patient's rights and drawing the legal framework for performing quality control procedures. Compared to the current legal framework, it is not sure that the proposal might improve any of these contributions to the patient's safety.

## Keywords

privacy – data protection – personal data – patient's safety

## Introduction

On 27 July 1990, the European Commission submitted to the Council a proposal of a directive on the processing of personal data.[1] The objective assigned to the directive was to facilitate the free movement of personal data within the European Community while maintaining a high level of protection for the citizens with regard to the processing of personal data. The proposal has been adopted on 24 October 1995 and is widely known since as the *privacy directive* or the *data protection directive*. It fixes the general rules applicable to the processing of personal data in all the Members States.

* Member of the Bar of Brussels; jean.herveg@unamur.be.

1 Com(90)314 final — SYN 287.

 | DOI 10.1163/15718093-12341322

The application of data protection rules begins with the identification of processing of personal data which falls under the scope of the directive.[2] Then, we have to determine the purposes for which the personal data are collected. These purposes must be specified, explicit and legitimate. And as we all know, the purpose principle is of the utmost importance in the application of data protection rules. Hence, personal data cannot be processed in a way incompatible with the purposes for which they had been collected. Personal data should be fairly processed in compliance with the purposes communicated to the data subject by the data controller. Personal data should also be lawfully processed. This refers to the compliance with special rules applicable to the processed data. In healthcare, lawfulness refers notably to the rules regarding professional secrecy. Furthermore, personal data must be adequate, relevant and not excessive in relation with the purposes for which they are processed. They also should be accurate and, where necessary, kept up to date. When the personal data processing purposes are achieved, data cannot be kept in a form which permits the identification of the data subject.[3]

The directive lists the situations in which a processing of personal data can occur.[4] With respect to this, it stipulates that processing of medical data is prohibited excepted in the enumerated situations.[5]

On the other hand, the data controller must provide the data subject from whom data relating to him or herself are collected with information on the processing of personal data.[6] The data subject has the right to access personal data relating to him.[7] At any time, the data subject may oppose the processing of personal data relating to him. In order to be successful, the claim must be grounded on compelling legitimate grounds relating to the data subject's particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the data controller may no longer involve those data.[8] In healthcare, this mechanism could be considered to prevent any reference to HIV-related information in the medical record in special circumstances.

The directive provides that everyone has the right not to be subjected to a decision which produces legal effects concerning him or significantly affects

2 See provision 3 of the Directive.
3 See provision 6 of the Directive.
4 See provision 7 of the Directive.
5 See provision 8 of the Directive.
6 See provisions 10, 11 & 13 of the Directive.
7 See provisions 12 & 13 of the Directive.
8 See Provision 14 of the Directive.

him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.[9] In healthcare, this refers, by instance, to the control of the patient's insurability by means of an electronic insurance card.

The data controller must ensure the confidentiality and the security of the processing of personal data.[10] The processing of personal data should also be notified by the data controller to the national supervisory authority.[11] Processing that are likely to present specific risks to the rights and freedoms of data subjects should be subject to prior examination.[12]

The national supervisory authority has the duty to keep a public registry with all the processing that have been notified.[13] This is one of the measures enabling the data subject to exercise his rights on the processing of personal data.

The transfer of personal data to a third country is subject to special rules.[14] In short, this kind of operation is prohibited except when the country of destination ensures an adequate level of protection for personal data.

Last but not least, the data subject must have access to appropriate judicial remedies. The Directive provides that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the Directive is entitled to receive compensation from the data controller for the damage suffered. The data controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.[15]

On 25 January 2012, the European Commission has issued a proposal for a general data protection regulation (COM (2012) 11 final) aiming at replacing the privacy directive. The fundamental ideas underpinning the proposal are the necessity to adapt the current legal framework to the development of new technologies and to put an end to existing disharmonies between national laws, while maintaining a high level of protection for the citizen.

9 See Provision 15 of the Directive. This right is not limitless.

10 See Provisions 16 & 17 of the Directive.

11 See Provisions 18 & 19 of the Directive.

12 See Provision of the Directive.

13 See Provision 21 of the Directive.

14 See Provisions 25 & 26 of the Directive.

15 See Provisions 22 & 24 of the Directive.

This article aims at opening a debate on the question of whether or not this proposal could enhance the patient's safety.[16] We suggest to discuss this question through the prism of the most important contributions that should be expected from data protection to patient's safety. Then we will try to see whether the current data protection directive succeeds in addressing each one of these expected contributions,[17] before considering whether the proposal could remedy to potential failures of the current data protection directive. The article will end underlining the issues that could have been missed by the proposal and that should be addressed.

In our view, data protection may contribute to the patient's safety on at least four major issues.

(1) Data protection should help creating efficient information systems which support the provision of the best healthcare possible to the patient, whether in hospital or in ambulatory care. It means that data protection should support the collection, the use, the transmission and the storage of medical data which are necessary to provide the patient with adequate state-of-the-art healthcare. In other words, data protection should not establish unjustified obstacles to the use of ICT in healthcare.
(2) Data protection should aim at increasing the informational quality of data processed in healthcare. In our view, ICT in healthcare should be an opportunity to raise the quality of the data used when providing healthcare to the patient.
(3) Data protection should support the patient's right to control the processing of data related to his health, notably when these data are initially or further processed for medical or scientific purposes. The patient's right to control the processing of his data includes mainly the right to get information about the processing, the right to consent to their processing and the right to access them. This way, the patient would have a better understanding of his health condition and he would also be in a better position to exercise his right of self-determination when receiving healthcare or when participating to medical research.

16 On this topic, see also the Directive 2011/24/EC on the application of patient's rights in cross border healthcare.

17 See the first report on the implementation of the data protection Directive (COM (2003) 265 final — 15 May 2003) and the communication of the Commission to the European Parliament and to the Council on the follow-up of the Working Group on a better implementation of the data protection Directive (COM (2007) 87 final — 7 March 2007).

(4) Data protection should state the conditions under which patient's data could be used for review mechanisms or for other quality control procedures.

## 1 Data Protection and Efficient Information Systems

When using ICT in healthcare, the data protection directive requires that the data controller has to pursue a specified, explicit and legitimate purpose when collecting, using, communicating or storing personal data concerning the patient in order to provide him with appropriate state of the art healthcare. It will be hard not to find a base to legitimate the processing of personal data in those circumstances. Regarding medical data, the ban to process them will be lifted thanks to the exception provided for the processing of personal data for medical purposes. The directive only requires specifically that the processing must be realized under the supervision of someone bound to professional secrecy or to any equivalent duty of secrecy. Of course, the use of ICT in healthcare will be subject to the general conditions regarding the lawfulness of the data processing. With respect to this, the level of security will obviously impact the legitimacy assessment and the analysis of the compatibility of any operation performed upon personal data.

As we can see, if the data controller uses state of the art ICT and complies with the general rules on the lawfulness of the data processing (quality principle, legitimacy requirement, information duty, right of access, right to object and confidentiality and security of the data processing, and notification to the national supervisory authority) — which are not extraordinary requirements —, the data protection directive creates no special obstacle to the use of ICT in healthcare.

But problems may arise from another side. The harmonization of data protection rules concerns only restrictions on personal data processing on the ground of protecting the rights and liberties of the data subject. Therefore, disharmonies can find a cause in legal aspects that are not been subjected to the harmonization. By instance, rules on professional secrecy may impose restrictions on the use of ICT in healthcare and may prevent some communication of personal data. Public health or social security requirements may impose the communication of various personal data to public bodies for quality control or for funding purposes. In both cases, this kind of national requirements may vary from country to country and even within a same country regarding the national distribution of powers. Of course, the data protection directive is not the cause of this kind of discrepancies between national legislations.

Their cause must be found in national laws and in the rules regarding the distribution of powers between the European Union and the Member States and within the Member States.

On the other hand, the data protection directive allows for questioning the legitimacy of using ICT in healthcare notably in terms of costs for the healthcare system. By instance, is it legitimate to implement costly and non-efficient ICT in healthcare when there is a huge funding deficit in healthcare? This approach allows us to demonstrate that the legitimacy requirement may help to oppose to the implementation of inefficient information systems in healthcare, which is, in our view, a good point in favor of the data protection directive.

However, there is one point of the directive which may cause difficulties in implementing ICT in healthcare. It is the ban on processing medical data. From a data protection point of view, this ban is considered as the best protection possible for the data subject. Where there is no processing, there is no risk for the data subject. But, from a medical point of view, it can be quite disconcerting. Indeed, it might be uneasy to explain to a health practitioner that the use of medical data is forbidden except when being in one of the situations listed in the data protection directive. Of course, one of these situations concerns the processing of medical data for medical purpose. But, nevertheless, the first principle is to oppose any processing. This might lead to some serious misunderstanding, especially when implementing new ICT in a non-friendly environment. Therefore, our suggestion would be to discuss the possibility to change the phrasing of the ban and to state that: "The processing of medical data may only occur under the direct order and constant supervision and monitoring of a professional healthcare practitioner for the following purposes (. . .)" and then to finish the provision with stipulating that "The processing of medical data is otherwise forbidden".

## 2 Data Protection and Data Quality

In our view, one of the major risks, besides the use of personal data for illegitimate purposes, lies in the wide dissemination of incorrect personal data. Therefore, one condition to allow for the free circulation of personal data is that the data controller must ensure the quality of the processed data. Somehow, strong requirements regarding data quality should be the normal counterpart to the possibility given to data controllers to process personal data.

As mentioned before, in the current state of the legislation, the quality principle implies that personal data must be fairly processed in compliance with the purposes indicated to the data subject by the data controller. Personal data

must be lawfully processed and the purposes for which the personal data have been collected must be specified, explicit and legitimate. Personal data cannot be processed in a way incompatible with the purposes for which they had been collected. Furthermore, personal data must be adequate, relevant and not excessive in relation with the purposes for which they are processed. Personal data also should be accurate and, where necessary, kept up to date. When the personal data processing purposes are achieved, data cannot be kept in a form which permits the identification of the data subject.

As we can see, the data quality principle is formally quite well established. But the question is whether or not it has been fully implemented, whether or not all its implications have been totally and completely exploited. Is it sure that we have used all the possibilities, all the opportunities offered by ICT in healthcare to improve the data quality and therefore the quality of the healthcare provided to the patient?

It is quite difficult to have an informed opinion on this matter due to the lack of enough exhaustive and serious studies on the topic. But, too often, it seems that ICT have just replaced the paper in the management of the patient's data. This raises the legitimacy of the use of ICT in healthcare. If it was only about that, was it worth to put the patient's rights and liberties in jeopardy?

In response to this issue, wouldn't be possible to strengthen the data quality principle by adding that the use of ICT in healthcare must improve the informational quality of the data used to provide the patient with adequate state of the art healthcare? Of course, it would imply to monitor the data quality.

*A minima*, shouldn't we consider that the processing of medical data is equivalent to a medical act subject to state-of-the-art rules? *A maxima*, shouldn't we consider to impose procedures when processing medical data?

In our view, the data protection directive should not be drafted only in a way to facilitate the selling of more ICT to hospitals or health practitioners. It should mainly aim at improving the quality of the healthcare provided to the patient based upon real and efficient and measurable requirements. The proposal of a general data protection regulation does not seem to bring anything new on this issue.

## 3 Data Protection and Patient's Rights on Data Processing

The data subject is entitled to get some information from the data controller about the processing of personal data. Therefore, at least, except when the data subject already has it, the data controller must provide the data subject with the following information:

(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing for which the data are intended;
(c) any further information such as
  – the recipients or categories of recipients of the data,
  – whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
  – the existence of the right of access to and the right to rectify the data concerning him,

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

The data subject has the right to consent to the processing of personal data, the right to access personal data concerning him and, in some circumstances, the right to oppose to the processing of personal data. He also has a right to judicial remedies in case of damages caused by a violation of data protection rules.

In our view, those rights contribute to the empowering of the patient in healthcare. When exercising them, the patient should have a better understanding of his health condition and he also would be in a better position to exercise his right of self-determination when being taken care of by a health practitioner or when participating in medical research.

We think that it is really important to strengthen the patient's rights about the processing of personal data. His rights are firmly stated in the data protection directive but it is not sure whether or not they are fully exploited in healthcare. The proposal for a general data protection does not bring anything new with respect to this. However, we could wonder whether or not the intervention of the national supervisory authority in an authorization scheme might lead to a weakening of the patient's control over his personal data. Indeed, in this case, it could be assumed that the control will be performed by the national supervisory authority instead of the patient. We could argue that this public body has more power and resources to perform the duty but in the same time it takes the things off the patient's hands. It is somehow contradictory with the empowering theory. Obviously, a better combination of both forms of control should be conceived.

From a practical point of view for the patient, we should consider to impose to the data controller a pro-active duty to send to the patient, on a regular base, an intelligible report of the medical data related to him and to organize a better communication between the healthcare practitioner and the patient: at the appropriate moment, the health practitioner should provide the patient

with the information that will be used when treating him. That could permit to avoid some misunderstanding in the transmission of some vital information regarding the patient's condition.

## 4 Data Protection and Quality Control Procedures

Alongside the quality principle, we are wondering whether there should be a more detailed legal framework when using ICT for review mechanisms and other quality control procedures.

Under the Privacy Directive, the ban to process medical data does not apply where the processing is required for the purposes of managing health-care services. Furthermore, subject to the provision of suitable safeguards, Member States may lay down, for reasons of substantial public interest, additional exemptions to the ban to process medical data, either by national law or by decision of the national supervisory authority. It is usually considered that review mechanisms and other quality control procedures should fall under the scope of health-care services management and reasons of substantial public interest. That being said, the Privacy Directive does not provide any other details on the matter which seems regrettable.

The proposal of a general data protection regulation seems more specific on this issue.

Provision 81.1(b) of provides that personal data concerning health could be processed for necessary reasons of public interest in the area of public health, such as ensuring high standards of quality and safety, inter alia for medicinal products or medical devices. It provides that this kind of processing should be based upon the law of the European Union or of a Member State which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests.[18]

Furthermore, Provision 81.2 provides that the processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, should be subject to the conditions and safeguards referred to in Provision 83.

18 Provision 81.3 gives the power to the Commission to adopt delegated acts for the purpose of further specifying other reasons of public interest in the area of public health as referred to in 81.1(b), as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in 81.1.

Provision 83 provides that personal data may be processed for historical, statistical or scientific research purposes only if it cannot be done with anonymous data and if the data enabling the attribution of information to the data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.[19]

In our view, these provisions of the proposal of a general data protection regulation cover the issue of the review mechanisms and other quality control procedures but they still lack precision. We are wondering whether or not review mechanisms and other quality control procedures shouldn't be regulated by a specific piece of regulation which would define more precisely the conditions to process personal data for these purposes? This question seems even more important regarding the development of the Big Data phenomenon.

## Conclusions

It can be said that the data protection directive contributes to the patient's safety on the four contributions that have been considered in this article. However we are not convinced that the ways in which data protection could contribute to the patient's safety have been fully exploited. We are not sure that the proposal of a general data protection regulation will add anything new or exceptional to this ascertainment.

Of course, the proposal offers a general legal framework for processing personal data and it cannot expected that it could cover each particularities of each domain covered by the data protection regulation. But, in the same time, the proposal, like the data protection directive, provides some very specific requirements on the processing of medical data. In other words, the proposal, like the directive, offers a general regulation but, in some aspects, it goes beyond and offers special rules dedicated to specific activities. This seems to be contradictory even if there are rational explanations for this situation.

19 Provision 83.3 allows the Commission to adopt delegated acts to specify the criteria and requirements for processing of personal data for the purposes referred to in 83.1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances. It is not sure that there could be any serious reasons to limit the data subject's rights. On the contrary, shouldn't be considered that the reinforcement of the data subject's rights are in order to balance the interference in one's right to respect for private life?

In any case, we are not convinced, at this point, that the proposal will succeed in meeting the real needs of the healthcare sector, especially regarding the issues raised by cloud computing services or by the big data phenomenon.

Perhaps the processing of medical data should be entirely regulated by a separated [additional or principal?] piece of legislation.

There are many other issues raised by the proposal of a general data protection regulation. The least of them is not the power distribution problem between the European Union and the Member States and the compliance with the subsidiarity principle. In our view, the European Association of Health Law is the most suitable place to discuss and to work on the topic of ICT in healthcare.