Study on Legal and Regulatory aspects of eHealth "Legally eHealth" : deliverable 2 : processing medical data : data protection, confidentiality and security

Herveg, Jean

Publication date:
2006

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

European Commission
Contract # 30-CE-0041734/00-55

Study on Legal and Regulatory Aspects of eHealth

"*Legally* eHealth"

DELIVERABLE 2

PROCESSING MEDICAL DATA: DATA PROTECTION, CONFIDENTIALITY AND SECURITY

Start Date:	**1st January 2006**
Commencement date of Contract:	**1st January 2006**
Duration:	**12 months**
Contractor:	**European Health Management Association**
Version:	**8.0 (Final)**

DOCUMENT LOG

Issue	Date	Comment	Author
	27/02/06	Legal analysis - first version	I. Vereecken, J. Herveg
	21/03/06	Case vignettes – addition of legal issues	D. Silber
	24/03/06	Case vignettes – analysis of legal issues – first version	J. Herveg
	02/04/06	Legal analysis – second version: addition of detailed legal references	I. Vereecken, J. Herveg
	03/04/06	Case vignettes – analysis of legal issues – second version	J. Herveg
	10/04/06	(project meeting) analysis of legal issues, adaptation of case vignettes	P. Wilson, C. Van Doosselaere, D. Silber, I. Vereecken, J. Herveg
	21/04/06	Case vignettes – second version	D. Silber
	27/06/06	Case vignettes – third version	D. Silber
	06/07/06	Legal analysis - third version Legal analysis of case vignettes - first version	I. Vereecken, J. Herveg
	10/07/06	(project meeting) finalisation of format, style and content	P. Wilson, C. Van Doosselaere, D. Silber, I. Vereecken, J. Herveg
	17/07/06	Legal analysis – fourth version Legal analysis of case vignettes – second version	I. Vereecken, J. Herveg
	21/08/06	Editing of full text	P. Wilson, C. Van Doosselaere
	1/9/06	Final text	
	27/4/07	Quality Review	Christian Dierks
8.0	30/05/07	Final release	C. Van Doosselaere

TABLE OF CONTENTS

PROCESSING MEDICAL DATA: DATA PROTECTION, CONFIDENTIALITY AND SECURITY

INTRODUCTION

eHealth applications[1], whatever their nature, will frequently involve the processing of information relating to an identified or identifiable patient. Such information is legally known as personal data and is subject to data protection legislation in the European Union.

In Europe, such data are protected by legal rules found in a number of legal sources. The purpose of this document is to guide the reader through the most important EU-level rules that will apply to handling and processing patient personal data. It will be useful to any person who, in the course of executing his or her job, collects, processes or treats information, from and about patients, that is stored in paper files or on a computer. This document will explain all the general duties that will apply to such a data handler and also the protection that it offers to patients. It should be noted, however, that this document looks at EU-level legislation[2]. Part of this legislation is not generally 'directly applicable' that is, it has to be transposed into national or regional level legislation, which will apply in a given European country.

However, despite small differences in the transposition and in the interpretation of the EU-level legislation between the European Member States, the basic principles of privacy of health related information are the same within the EU. As in ancient codes such as the Hippocratic Oath, all healthcare workers are bound by legislation that requires them to respect the autonomy and privacy of patients.

The general legal principle of data privacy, similar to that found in the Hippocratic Oath, was first established by the Council of Europe in 1981 and further developed in Directive 95/46/CE of the European Union. This is the single most important EU-level legal statement about data privacy and confidentiality, including medical and other sensitive data. While some national and regional variations may arise, the basic principles as explained in this document will apply to all 27 European Union Member States.

This document is divided into four parts:

Part I: A summary description of the key principles of EU level Data Protection legislation.
Here you will find an outline of the key principles of the legislation with some healthcare based examples.
Part II: A detailed step-by-step analysis of that Directive.
The analysis includes a description of all the relevant articles of legislation as well as links and references to the source documents.
Part III: A series of case vignettes that show the way in which the legislation works.
The fictional cases will show examples of eHealth applications and explore the data protection duties that they imply for the healthcare providers and other actors.
Part IV: A Source Reference list.
Here you will find links and reference to all the legal source documents discussed in parts one, two and three.

[1] See introduction - general 'what is eHealth' section - create hyper link later
[2] See discussion of EU Legislation in Introduction – create hyperlink later

PART I: KEY PRINCIPLES OF DATA PROTECTION IN THE EUROPEAN UNION

A. What is the purpose of the Data Protection Directive?

The primary purpose of the EU Directive on Data Protection (95/46/EC) is to protect the fundamental rights and freedoms of natural persons. Natural persons are 'real' people, as opposed to legal persons such as companies or societies. Within the legislation, such a natural person is referred to as a data subject – in other words, the person to whom the personal data relate.

However, the Directive has a further purpose: to allow the free movement of personal data within the European Union in the context of the internal market. On the one hand, therefore, its object is to protect the privacy of individuals and on the other hand, it is to allow a freedom of movement of data across the European Union in order that the internal market might prosper.

The clue to the duality of purpose in the Directive is found, in fact, in the Directive's full and proper name: Directive on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data. Two particular issues are central to understanding the impact of the Directive on medical practice: first, the definition of 'personal data' and second the nature of 'processing'.

The central concept behind the enactment of the Data Protection Directive is that the transposition of the Directive into national laws in all the Member States will harmonise the EU national legislations so that a broadly similar level of protection of rights and freedoms of natural persons regarding the processing of their personal data exists across all Member States. This harmonisation is to remove the need for a Member State to restrict cross-border flow of data, and by implication cross-border trade, because of a perceived lack of data protection in another Member State. For this reason, Member States are normally not allowed to provide for a restriction or prohibition on data flows between Member States in their transposition of the Directive.

B. To what types of data does the Directive apply?

The Directive provides a general framework for the protection of privacy with respect to the processing of personal data in its widest sense. Note here the protection offered by 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. In that context it goes further than the protection of the *intimacy* of the natural persons i.e. generally speaking their private life, because the definition of personal data covers *all data related to a natural person*, whether the context of such information is the private, public or professional life of the individual.

In order to establish if data are covered by the Directive, one must therefore first ask if the data are such that they 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). Thus, the laboratory result of a

blood sample test giving the count of various markers in the blood will be covered by this legislation if the identification of the originator of the blood is possible using reasonable means. By example the Directive applies if the laboratory results are stored with coded identifiers, such as a patient number. 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, even by or with the help of a third person, then the data is considered as identifiable and therefore in the scope of the Directive. If the information refer 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. The full detail of the finer points of this interpretation of identifiable data is explored in Part 2 below.

C. 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 pursued by 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 regarding the purpose of the processing of personal data.

But some data are considered as sensitive and therefore require a 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.

Moreover some data processing presents special risks to the rights and freedoms of the data subjects. These data processing have to be checked prior their start.

D. Who has data protection duties?

The data protection rules are addressed primarily to the **data controller**. This person decides the purpose and the means of the processing and has the legal duty to ensure that data are handled appropriately. In most professional cases, this will be a senior staff member who is named as the person responsible for data collected and stored by an organisation.

In the case of small companies or self-employed individuals (such as many General Practitioners (GPs)), the data controller will generally be the person who has legal and tax liability for the organisation. It should be noted that organisations need not be businesses or legally constituted to be covered by the legislation. Thus, a disease self-help group will fall within the legislation and its data controller will be its president or other lead person. Natural person and legal person may be the data controller (i.e. processing made by self-employed practitioners).

E. What are the main duties of a person who controls personal data?

Any personal data that the controller needs to process for the purposes of his or her professional activity must meet certain levels of quality and comply with different principles concerning data collection and processing as well as principles concerning data processing.

1. DUTIES CONCERNING DATA COLLECTION AND PROCESSING

The data must be collected for specified, explicit and legitimate purposes. This principle requires that, prior to process personal data, the controller has to define clearly and precisely the purpose(s) for which the data are to be processed. Moreover, the processing should be transparent. The data controller will therefore have to provide the relevant national data supervisory authority (notification duty) and the data subject (information duty) with certain information regarding the processing.

The purpose of the processing must be legitimate. The Directive lists the general conditions under which the processing will be presumed as legitimate. According to the Directive National law will define what types of data processing are legitimate. However in each case the interests in the data processing must outweigh the interests of the data subject in excluding the processing of the data. For example, in a health setting, the data subject will have a greater interest in his or her health data being shared with appropriate professionals if the sharing of the health information will allow better and safer healthcare delivery.

The controller must only process personal data for the purposes for which the data were collected and cannot further process the data in a way incompatible with the initial purpose. A controller wishing to process the data for purposes distinct from the original purposes will have to satisfy the conditions for the re-use of personal data. As a general rule softer rules for the re-use of data for statistical, historical or scientific purposes have generally been provided in Member States legislations.

Thus, a doctor who may share patient identifiable data with another doctor for the purposes of treating the patient may share that same information with another healthcare professional for the purpose of conducting medical research if that purpose was originally given as one of the final uses of the data or if this is compatible with the latter (especially if the data subject has given his or her consent to the communication) or if appropriate safeguards are met for processing personal data for medical research viewed as a scientific purpose (i.e. reasonable steps are taken to hide the true identity of a data subject). If the personal data are anonymised by the doctor there is no problem to communicate the anonymous data to a third party for scientific purpose including medical research safe for other special rules in National Law (i.e. medical secrecy).

The data must be processed fairly and lawfully and therefore should be processed in accordance with the law(s) including good practices. Moreover, the type and quality of personal data to be collected must be carefully selected so that it is adequate for the stated purpose but not excessive. Thus, if a researcher collects data in order to carry out a specified research project, he or she may not collect and process other data which are not necessary for the study in hand but might be useful at some later date.

2. DUTIES RELATING TO DATA STORAGE

Once the data are collected, the controller must keep them accurate and, where necessary, keep them up-to-date. Personal data should be stored for a limited period of time and must be erased, rendered anonymous or destroyed when the pre-defined purpose of processing has been achieved.

According to the Directive, data subjects benefit from rights in order to allow them to have a certain control over the information that is held about them. For this purpose, data subjects have access rights to the data, which allow them to request specific information about their own personal data; the right to ask for data to be rectified when they are incomplete or inaccurate; and under some conditions, the right to object to the processing. On the basis of these duties most European Union countries have introduced legislation that allows patients access to their medical records and allows patients to demand a rectification of a record.

Amongst the duties imposed on the data controller, he or she has the responsibility to protect the personal data he or she holds and therefore to take technical and organisational measures ensuring their security and confidentiality. A data controller may pass data to a third party to act as a data processor to process the data on his or her behalf but the data controller will have to comply with some requirements in order to be allowed to do so. In a medical setting one of the key legal issues affecting the data processor is that he or she must have a legal or a contractual duty to maintain data confidentiality. 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 he or she is also legally responsible in case of any breach of data confidentiality.

F. Are medical data treated differently by the Directive?

All the principles described above are general principles that may alter very slightly when the data are regarded as especially sensitive. Data concerning a person's health, religion, trade union activity as well as data revealing racial or ethnic origin and judicial information are amongst the data regarded by the Directive as especially sensitive and therefore subject to special rules. For this reason, data that are capable by their nature of infringing fundamental freedoms or privacy of the data subject should normally not be processed.

The ban on processing sensitive or medical data aims to ensure the respect of the fundamental rights and freedoms of the data subject regarding the processing of his or her medical data. The principle of the ban is not absolute: in some specific circumstances, the processing of sensitive data is possible. Thus, all EU countries hold by principle that medical data may not be collected or processed unless to do so is for certain purposes and following certain guidelines, including notably:

- the explicit informed consent of the data subject ;
- 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;
- for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, 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.

PART II: DETAILED ANALYSIS OF THE LEGAL TEXTS

A. Key concepts

1. PERSONAL DATA (D., ART. 2.A)

Personal data are any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, using reasonable means, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

To be considered as personal data the data:

(a) might concern any information regarding the data subjects such as their name, their e-mail address, an opinion, a fact, a measurement, a sound or an image, or their personal circumstances, whether these relate to the data subject's private, professional or public life;
   - In the case of medical data this could include a record of a medical intervention, a diagnosis, a prescription, a genetic profile, an x-ray, an echogram, a blood count… and so on;

(b) must relate to natural persons. Data strictly relating to companies, public bodies, *etc.* are not personal data. However, in some countries (e.g., Austria, Luxembourg and Italy), the data related to companies are protected as personal data;

(c) might concern persons that are alive or dead at the moment of the processing. However, in some of the Member States (like in Ireland, Sweden and United Kingdom), personal data only concern alive persons;

(d) must allow the direct or indirect identification of the data subject.
   - Data allowing *direct identification* are data that can be easily related to a data subject and reveal their identity. This is the case of data such as the name, address, date of birth or even genetic data which, when combined with one another, allow identification with a small margin of doubt.
   - *Indirect identification* requires further steps to make a link between a specific person and the data being processed. Therefore, the fact that data are not directly related to a person does not necessarily imply that they do not constitute personal data.
   - In the Directive and in most European countries, this concept is applied *in abstracto*; that is, the possibility of identifying a person through the data is defined by the mere existence of a possibility to establish a link between the data and a person. This possibility of linking could be made by the data controller or even by a third person. The logic is thus applied that if something can be rendered anonymous or pseudonymous by a process, such a process could be reversed using reasonable means, therefore these data are nevertheless identifiable. In fact these data are coded data.
   - In some Member States, such as the United Kingdom, Ireland, Austria and the Netherlands, this assessment is made *in concreto*; that is, taking into account only the information that is, or is likely to be, in the possession of the controller, to identify the data subject through the data.

2. ANONYMOUS DATA

Anonymous data are being defined as data that cannot be qualified as personal data, since they do not (any more) allow direct or indirect identification of the data subject using reasonable means.

Anonymous data are not subject as such to data protection requirements. However, note that the definition of a given piece of data as anonymous is not necessarily straightforward (see above). Furthermore, the processing carried out to render data anonymous is considered to be a processing of personal data. Thus the process of anonymisation of data is covered by the data protection requirements.

To escape the legal requirements arising out of the processing of personal data, the processed data must already be rendered anonymous. Until the moment the data are rendered anonymous, the controller must comply with all the legal requirements for the processing of personal data. The question to address is to know if the operation of anonymisation is compatible with the purpose of the initial data processing and how this anonymisation should occur (should it be done by the initial data controller or by a third party? Using what technique?). But save for exceptional circumstances and special rules from national laws (i.e. medical secrecy when anonymised by a third party) the operation of anonymisation by the data controller should be compatible in any case. Regarding this question it should be added that in any case personal data have to be anonymised at least at the end of the data processing.

Thus, in a medical setting, a researcher wanting to carry out research on anonymous data outside the application of the Data Protection legislation would need to acquire the anonymised data from an authorised controller who had already anonymised the data in such a way that it would be reasonably impossible for the researcher and for any other person to re-identify the data.

3. SPECIAL CATEGORIES OF DATA (D., ART. 8)

This term, used in the Directive, refers to specific categories of data revealing sensitive information about a data subject. Those data are subject to more restricted rules than 'normal' personal data.

Special categories of data are:

- Sensitive data
  - data revealing racial or ethnic origin
  - data revealing political opinions
  - data revealing religious or philosophical beliefs
  - data revealing trade-union membership
- Medical data
  - data concerning health (including mental health) or sex life
- Judicial data
  - data relating to offences, criminal convictions or security measures
  - data relating to administrative sanctions or judgments in civil cases

4. GENETIC DATA

Genetic data is defined by the Recommendation (97)5 of the Council of Europe as all data, whatever type, concerning the hereditary characteristics of an individual or concerning the pattern of inheritance of such characteristics within a related group of individuals. It also refers to all data on the carrying of any genetic information (genes) in an individual or genetic line relating to any aspect of health or disease, whether present as identifiable characteristics or not.

Genetic data are generally considered as medical data but they are not always. They may be subjected to more restrictive conditions of processing.

5. PERSONAL DATA PROCESSING (D., ART. 2.B)

The concept of processing is very broad. It applies to any operation or set of operations that are performed upon personal data, whether or not by automatic means. Data processing is considered to be the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of personal data.

The application of data protection legislation is limited to automated processing and to non-automated processing that, nevertheless, forms part of a filing system or is intended to form part of a filing system.

6. PURPOSE

The term 'purpose' is a key concept in data protection regulation, defining the scope of the processing and assessing whether processing is lawful or not. The purpose refers to the aim pursued by the specific processing of personal data.

7. CONTROLLER (D., ART. 2.D)

The controller is the natural or legal person who, alone or jointly with others, determines the purposes and means of the processing of personal data.

8. DATA SUBJECT

The data subject is generally defined as the person to whom the personal data relate.

9. PROCESSOR (D., ART. 2.E)

The processor is the natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller. This will typically be a specialized third-party company entrusted by the controller to conduct the technical aspects of the processing, such as the sorting or the combination of the personal data.

The employee of the controller in charge of the security and management of the computer system is not to be considered as a processor.

10. THIRD PARTY (D., ART. 2.F)

The third party is any natural or legal person, public authority, agency or any other body other than :

- the data subject,
- the controller,
- the processor
- and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.

11. RECIPIENT (D., ART. 2.G)

The recipient is a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.

12. DATA SUBJECT CONSENT (D., ART. 2.H)

Any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed.

13. PERSONAL DATA FILING SYSTEM (D., ART. 2.C)

The processing operations covered by data protection legislation are not limited to automated processing such as electronic files or databases, but also include the non-automated processing (manual paper file) that forms part of a filing system or is intended to form part of a filing system.

A filing system is any structured set of personal data that are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis. Therefore, a manual processing will be covered by data protection legislation as soon as this is structured according to certain criteria.

14. SUPERVISORY AUTHORITY (D., ART. 28)

Independent national public authorities are responsible for monitoring the application of the national data protection legislation within its territory.

The supervisory authority received the notification of the processing prepared by the controller and has notably the power to make investigation, to engage legal proceedings and to deliver opinions.

B. Scope of the data protection legislations

According to the European Directive as well as to the Convention n°108 of the Council of Europe, data protection principles apply equally to the public and private sectors.

The European Directive applies to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. Manual processing that does not form part of a filing system or that is not intended to form part of a filing system is not covered by data protection Directive (D., art. 3.1).

Processing of data carried by a natural person in the course of a purely personal or household activity is not governed by data protection laws either (D., art. 3.1.).

C. Lawfulness of the processing: Conditions regarding the legitimacy of the processing

1. NON-SENSITIVE DATA

To be qualified as legitimate, the processing has to correspond to one of the social justifications laid down by law. The controller should ensure that the processing is covered by one of these justifications (D., art. 7) :

(a) the data subject (or his or her legal representative) has unambiguously given his or her consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except when such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

To rely on this last justification (f), the controller should:

(i) identify the interests being pursued by the processing,
(ii) determine whether the interests are legitimate, and
(iii) verify that the effect on the rights and liberties resulting from the processing of the data subject is not disproportionate, so that these rights and liberties should prevail over the interests of the controller. When assessing the existence of such prevalence, the controller should have regard to the interest of the data subject in not having his or her data processed as well as to any potential damage or distress that could be caused to the data subject because of the processing of his or her data. Moreover,

when the purpose(s) can be achieved by different schemas of processing, the controller should always prefer the one that causes fewest damage or inconvenience to the data subject.

2. MEDICAL AND OTHER SENSITIVE DATA

The processing of medical data is subject to restrictive conditions. In principle, their processing is prohibited, but may be permitted under specific circumstances (D., art. 8) :

(a) the data subject has given his or her *explicit consent* to the processing of those data, except when the national law of a Member State provides that the prohibition may not be lifted by the data subject's giving his consent; or
(b) 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; or
(c) processing is necessary to protect the vital interests of the data subject or of another person when the data subject is physically or legally incapable of giving his or her consent; or
(d) 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; or
(e) 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 when those 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.

Moreover, the European Directive offers the opportunity for the Member States to add exemptions for reasons of substantial public interest that could be subject to specific safeguards, like the authorisation of the national supervisory authority. This section may allow for instance, the adoption of a national exemption for scientific research or for social security reasons. This does not exclude the possibility to process medical data for scientific purpose with the consent of the data subject.

According to Recommendation (97)5 of the Committee of Ministers to Member States on the protection of medical data, adopted on 13 February 1997, if medical data have been collected for preventive medical purposes or for diagnostic or therapeutic purposes with regard to the data subject or a relative in the genetic line, they may also be processed for the management of a medical service operating in the interest of the patient, in cases when the management is provided by the health care professional who collected the data, or when the data are communicated in accordance the rules relating to the communication of medical data.

D. Lawfulness of the processing: Conditions regarding the quality of the data

As already mentioned the data must be processed fairly and lawfully and be collected for specified, explicit and legitimate purposes.

Any personal data that the controller needs to process must meet a certain level of quality and comply with the following principles:

1. THE DATA MUST BE PROCESSED FAIRLY AND LAWFULLY (D., ART. 6.1.A)

To be fair, the data processing must be transparent to the data subject. This involves the data controller complying with the information duty and with the notification duty. The data controller should also respect the principles of good practice described in codes of conduct.

To be lawful, the processing must respect the data protection laws but also other legal requirements (for instance, special legal texts relating to the medical sector, such as medical secrecy) including good practices.

2. THE DATA MUST BE COLLECTED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES (D., ART. 6.1.B)

The data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.

The controller must precisely define the purpose of the processing and communicate it to the data subject (information right) and to the national supervisory authority (notification duty).

The purpose of the data processing must be legitimate, meaning that the interests in the processing pursued by the data controller must outweigh the interests of the data subject in excluding their data from the processing (see the list of legitimate purposes proposed by the Directive).

When assessing this, the controller should have regard to the interests of the data subject in not having his or her data processed, as well as to any potential damage or distress that could be caused to the data subject because of the processing of this data. Moreover, when the purpose(s) can be achieved by different methods of processing, the controller should always prefer the one that causes least damage or presents less inconvenience to the data subject.

The data may be used only for the initial purpose and should not be re-used in a way incompatible with the initial purpose. Generally speaking, the purpose of the new processing has to be compared to the initial one(s) in order to assess whether there is a close relationship between them. A new purpose that is clearly different from the initial one(s) is considered to be incompatible. When assessing whether the further processing or operation is compatible with the initial purpose(s), the controller shall also have regard to the context, the general philosophy of the secondary processing, as well as any other relevant criteria like whether the further processing will be conducted by a third party or not, the existence of a law that authorizes the second processing etc.

If not compatible per se with the initial purpose further data processing for historical, statistical or scientific purposes will be compatible if the appropriate safeguards laid down by the Member State are met (D., art. 6.1.b) or if the data subject consent to the further processing. The controller must refer to the relevant national law to know these safeguards that could vary from one Member State to another.

3. THE PERSONAL DATA MUST BE ADEQUATE AND RELEVANT AND CANNOT BE EXCESSIVE (D., ART. 6.1.C)

The data must be useful and necessary for the declared processing purpose. It is forbidden to collect or make use of irrelevant data, which are not pertinent or necessary for processing purpose. The controller should therefore avoid the use of personal data when purpose can be achieved without it. Furthermore, even when the work can only be performed by the processing of personal data, the controller should seek to keep the use of these data to the minimum necessary.

Additionally, the data cannot be excessive, meaning that they cannot create a disproportionate risk of undermining the data subject's interests. Useful data that are not indispensable for the purpose have to be considered as excessive.

4. PERSONAL DATA MUST BE ACCURATE AND, WHEN NECESSARY, KEPT UP TO DATE (D., ART. 6.1.D)

The controller has to take all reasonable means to fulfil this duty consisting in not processing erroneous, incomplete or obsolete data. If the controller knows or should have known that the data are not accurate, they must be erased or rectified.

5. THE PERSONAL DATA SHOULD BE STORED FOR A LIMITED PERIOD OF TIME (D., ART. 6.1.E)

Personal data must be kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the data were collected or for which they are further processed. As soon as the purpose can be achieved without personal data, the need to conserve such data must be considered to have ended and therefore, the data should be rendered anonymous or destroyed.

The Directive authorizes the Member States to allow the storage of data for a longer term provided that this is in order to use the data exclusively to carry out scientific, historical or statistical purposes provided for appropriate safeguards. Most national laws have provided for such authorization.

The Recommendation (97)5 of the Committee of Ministers to Member States on the protection of medical data, adopted on 13 February 1997 also authorizes longer storage in the interest of public health, to enable the controller to defend or exercise a legal claim. When a longer storage is possible, security measures should ensure the correct conservation and security of the data.

E. Respect the rights of the data subject

The data subject is generally granted certain rights with regard to the processing of his or her data: a right of information, a right of access to the personal data, a right to request that the data be corrected, and a right to object to the processing of the data under specific circumstances.

The controller should therefore anticipate the likely exercise of these rights, and take the necessary technical and organisational measures to ensure the effective exercising of these rights by the data subjects. This means in practice that data must be available in a format that can be reproduced by printout and read by the naked eye.

1. RIGHT OF INFORMATION (D., ART. 10)

The data subject (or his or her legal representative) must be in a position to learn of the existence of a processing operation and therefore, the controller must give some information about the processing to the data subject.

The controller will have to provide at least the identity (name, address, denomination or trade name, for example) of the controller and of his or her representative (if any), a description of purposes of the processing. Some additional information should also sometimes be given, such as the categories of data concerned, the recipients or categories of recipients of the data, the existence of the right of access to and the right to rectify the data concerning him or her, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply.

The additional information will have to be given if, having regard to the specific circumstances in which the data are collected, it is necessary to guarantee fair processing in respect of the data subject. The controller will have to assess, on basis of the circumstances and characteristics of the processing, whether or not additional information needs to be provided to the data subject. The processing of sensitive data or medical data normally requires the provision of the further information.

Recommendation (97)5 of the Committee of Ministers to Member States on the protection of medical data, adopted on 13 February 1997, states that when the processing relates to medical data, the controller must also provide information about the individuals or bodies from whom they are or will be collected. In the case of genetic analysis, the data subject should be informed about the objectives of the analysis and the possibility of unexpected findings.

The timing of information delivery as well as the possible exemption to this right depends on the type of collection of data. Indeed, personal data can either be obtained directly from the data subject (primary collection) or obtained from a distinct alternative source of data (secondary collection).

In the case of genetic analysis, the information should be given before a genetic analysis is carried out.

a. Primary collection

When the data are collected directly from the data subject, the information should be provided at the time the data are collected. When medical data are collected for medical emergencies, data necessary for the medical treatment may be collected prior to the information.

The duty of information does not apply where the data subject has already been informed, or already knows this information.

b. Secondary collection

When the personal data have not been obtained directly from the data subject, the new data controller should, before considering how to process these personal data or when to inform the data subject, assess whether they comply with the requirements for the re-use of such data.

The new data controller has to inform the data subjects about any secondary collection at the latest at the time of recording, or if disclosure to a third party is anticipated, no later than the time when the data are first disclosed.

The duty of information does not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. Disproportionate effort may result when it is impossible to reach or contact data subjects (for example, when the new data controller cannot easily obtain their addresses) or when contacting all the data subjects can only be done at great expense, which is disproportionate in comparison with the risk of infringing the rights of the data subjects.

2. RIGHT OF ACCESS (D., ART. 12)

Every data subject has the right to request specific information about his or her own personal data processed by the controller. When medical data are processed, the data subject may request from a health care professional to exercise his or her access right.

Upon request, the controller will have to provide the data subjects with the following information without constraint at reasonable interval and without excessive delay or expense:

- whether or not data relating to them are being processed by the controller,
- the purpose of the processing,
- the categories of data and the data processed,
- the recipients or categories of recipients to whom the data are disclosed,
- communication of the processed data in an intelligible form,
- the source of the data,
- knowledge of the logic behind the data processing.

Access rights may be refused if the processing is made for 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. However, such exemption from providing access may be granted under the conditions that there is clearly no risk of breaching privacy of the data subject, and the data are not used in order to take measures or decisions regarding any particular individual (D., art. 13.2).

The access to medical data may be refused if the national law provides for such additional exemptions (D., art. 13.1) i.e. :

- it is in the interest of protecting state security, public safety or it concerns criminal matters; or
- knowledge of the information is likely to cause serious harm to the data subject's health; or

- the information on the data subject is also revealing information on third persons or if, with respect to genetic data, this information is likely to cause serious harm to consanguine or uterine kin or to a person who has a direct link with this genetic line.

3. RIGHT OF RECTIFICATION (D., ART. 12)

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. 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 consent of the data subject.

In addition, if the controller has disclosed the data to third parties, the controller has to notify them about any corrections, erasure or blocking carried out. The notification to a third party does not have to be performed if it proves to be impossible or involves a disproportionate effort.

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.

4. RIGHT TO OBJECT (D., ART. 14)

The data subject has the right to object to the processing of his or her data and, where there is a legitimate objection, the controller may no longer process those data or communicate the data to recipients.

According to the Recommendation (83)10 of the Committee of Ministers on the protection of personal data used for scientific research and statistics, adopted on 23 September 1983, when the processing is made for scientific or statistical reasons, the data subject may withdraw his or her collaboration. It this hypothesis, the data subject should be entitled to ask for the erasure of the data collected.

F. Duties of the controller

1. NOTIFY THE NATIONAL SUPERVISORY AUTHORITY (D., ART. 18 - 19)

In order to ensure transparency around the existence and scope of any processing, the controller is required, prior to carrying out the processing, to provide the relevant national supervisory authority with certain pieces of information regarding the processing. The content of the notification will normally be accessible to the data subjects or third parties.

The notification will generally cover the identity of the controller, the purpose of the processing, the categories of data subjects, the recipients, and the transfers to third countries. The exact content of the notification is defined by the applicable national law, and further specified by National Data Protection Authorities.

2. ENSURE THE CONFIDENTIALITY AND SECURITY OF THE PERSONAL DATA (D., ART. 16 - 17)

In order to protect the confidentiality of the data processing, the Directive provides that any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

To ensure the security of the data processing, the controller must implement appropriate technical and organisational measures to protect personal data against, for example, 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.

The appropriate level of protection to be ensured depends of the state of the art, the cost of implementation, the risks represented by the processing, and the nature of the data to be protected (for example, sensitive data, like medical data require the highest protection).

An example of an organisational measure would be the appointment of a data protection officer in charge of data protection issues. Technical measures include back-ups, restricted access to the database to authorized persons, and the use of software protecting the system against viruses or hacking.

The importance of protecting medical data has been stressed in 1997 by the European Court of Human Rights in the cases M.S. v Sweden and Z v Finland: "The confidentiality of health data is a vital principle in the legal systems of the contracting parties of the convention".

The Recommendation (97)5 of the Committee of Ministers to Member States on the protection of medical data gives some examples of measures that could be taken when medical data are processed:

- control to entrance to installations in order to prevent any unauthorized person to have access to the data;
- control of data media in order to render it impossible to be read, copied, altered or removed by unauthorized persons;
- memory control in order to prevent any unauthorized entry of data to the information system or any unauthorized consultation, modification or deletion of the data;
- access control for the purpose of security and to put in place a selective access to the data – a separation should be made on identifiers and data relating to the identity of persons, administrative data, medical data, social data and genetic data;
- control of communication for giving the possibility to check and ascertain to which persons or bodies data can be communicated by data transmission equipment;
- control of data introduction for giving the possibility to check and establish *a posteriori* who has had access to the system and what personal data were introduced, when and by whom;

- control of transport to prevent unauthorized reading, copying, alteration or deletion of data during communication of data or transport of data media;
- availability control to safeguard data by making security copies.

Moreover the controller should appoint a person responsible for the security of the information system and for the data protection.

Intervention of a processor

If the controller entrusts part of the processing to a (sub-) processor, he or she should ensure that this processor provides sufficient guarantees on technical security measures and organisational measures governing the processing to be carried out in compliance with those measures. Moreover, the processing of data must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that (1) the processor shall act only on instructions from the controller and that (2) the appropriate technical and organizational measures shall also be incumbent on the processor.

In view of keeping proof, the parts of the contract or the legal act shall be in written form or another equivalent form.

G. Communication of data to third parties

The Data Controller may not communicate personal data to third parties unless the transfer or disclosure of personal data is a normal operation in the considered data processing or is a compatible further operation. As explained above, the controller have to check whether or not this transfer or disclosure falls within the scope of the initial purpose or is compatible with this purpose, in order to determine whether or not he or she can lawfully transfer or disclose the personal data within the borders of the European Union.

Anonymous data can be transferred without being subject to specific requirements.

Specific conditions for medical data

Medical data should not be communicated unless the following conditions are fulfilled:

- The medical data are relevant for the purpose of the communication; *AND*
- The recipient of the communication is subject to confidentiality rules equivalent to those incumbent to health care professionals, *AND*
- *EITHER* The communication is authorized by the law and is made for one of these reasons:
    - public health reasons,
    - prevention of a real danger or suppression of a specific criminal offence,
    - another important public interest,
    - protection of the rights and freedoms of others,
    - protection of the data subject or a genetic relative,
    - safeguarding the vital interest of the data subject or a third person,
    - fulfilment of a specific contractual obligations,
    - establishing, exercising or defending a legal claim;

- *OR* the data subject (or his or her legal representative, or an authority) has given his or her explicit consent
- *OR* the data subject (or his or her legal representative, or an authority) has not explicitly objected to any non-mandatory communication, if the data have been collected in a freely chosen preventive, diagnostic or therapeutic context, and if the purpose of the communication, in particular the provision of care to the patient, or the management of a medical service operating in the interest of the patient, is not incompatible with the purpose of the initial processing.

H. Transfer of personal data to non-EU (and non-EEA) countries

The transfer of personal data outside the European Economic Area (EEA) is governed by specific conditions that need to be met in addition to the requirements for the transfer of personal data to third parties.

The transfer of personal data to a recipient located in non-EEA countries is allowed if the country of destination does ensure an adequate level of protection (D., art. 25.1). Some countries (such as Argentina, Isle of Man, Guernsey and Switzerland) have been acknowledged by the European Commission as ensuring an adequate level of protection. The transfer of personal data to US companies that adhered to the US Department of Commerce's Safe Harbour Privacy Principles is also allowed. The European Commission also allows the transfer of personal data to recipients in Canada subjected to the Canadian Personal Information Protection and Electronic Documents Act (PIPED Act).

The Directive provides with some exemptions to the prohibition of transfer of personal data to countries not offering an adequate level of protection. These exemptions are the following:

(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
(c) 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; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

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 where the controller adduces adequate safeguards with respect to the protection of the privacy, fundamental rights and freedoms of individuals, and as regards the exercise of the corresponding rights. Such safeguards may result, in particular, from appropriate contractual clauses.

The European Commission decided that an adequate level of protection could, in particular, be achieved through a contract between the sender and the recipient of the personal data. The European Commission proposes standard contractual clauses that ensure an adequate level of protection.

Specific conditions for medical data

The Recommendation (97)5 of the Committee of Ministers to Member States on the protection of medical data establishes additional rules for the transfer of medical data to a country that does not have an equivalent protection:

- The person responsible for the transfer should indicate to the recipient the initial purpose of the processing as well as the persons or bodies to whom the data may be communicated; and
- The recipient should honour the purpose he or she accepted and not communicate the data to other person or bodies than those indicated by the person responsible for the transfer.

I. Additional specific rules for the processing of medical and genetic data

Some specific rules relating to the processing of medical data have been proposed by the Council of Europe within the Recommendation (97) 5 of the Committee of Ministers to Member States on the protection of medical data, adopted on 13 Feb. 1997.

The processing of medical data should be carried out only by health care professionals or by individuals or bodies working on behalf of health care professionals and who are subject to confidentiality rules equivalent to those incumbent on health care professionals.

Medical data must normally be obtained from the data subject. It is possible to obtain such data from other sources if some conditions are respected.

Medical data should not be communicated to third parties unless some conditions are respected.

Processing of genetic data

The recommendation (97)5 of the Committee of Ministers to Member States on the protection of medical data establishes specific rules concerning the processing of genetic data:

(a) Genetic data collected and processed for preventive treatment, diagnosis or treatment of the data subject or for scientific research, should only be used for these purposes or to allow the data subject to take a free and informed decision on these matters.
(b) Processing of genetic data for the purpose of a judicial procedure or a criminal investigation should be the subject of a specific law offering appropriate safeguards.
(c) The data should only be used to establish whether there is a genetic link in the framework of adducing evidence, to prevent a real danger or to suppress a specific criminal offence. In no case should they be used to determine other characteristics which may be linked genetically.

(d) For purposes other than those provided for in articles 4.7 and 4.8, the collection and processing of genetic data should, in principle, only be permitted for health reasons and in particular to avoid any serious prejudice to the health of the data subject or third parties.
(e) However, the collection and processing of genetic data in order to predict illness may be allowed for in cases of overriding interest and subject to appropriate safeguards defined by law.

J. Other specific rules for the processing of personal data for scientific research and statistical activities

The Recommendation (83)10 of the Committee of Ministers on the protection of personal data used for scientific research and statistics proposes different principles for the processing of personal data for research or statistics purposes:

(a) When it is possible, research should be undertaken with anonymous data. However, if this requirement would make the research impossible, personal data may be used. In this case, when medical data are involved, specific conditions are proposed by the Recommendation (97) 5 of the Committee of Ministers to Member States on the protection of medical data, adopted on 13 Feb. 1997.
(b) Personal data may not be used for another purpose than this research and could not be used to make decision or to take any action directly affecting the data subject. Moreover, the personal data may not be used for another research project substantially different in its nature or objects from the initial one, except the data subject gave his/her consent.
(c) The personal data may not be published unless the data subject has given his consent for this publication and the national law allows it.

PART III: CASE VIGNETTES

Introduction

We have so far provided a general overview of the principles of data protection in the European Union and their application to medical data (Part I) and a detailed analysis of the key legislation (Part II). Part III will look at those principles and definitions in practice by using a series of fictional cases.

Each case vignette has been constructed on the basis of reported case histories to outline the way in which the data protection rules might be applied in practice. The case vignettes are not 'real' cases as such but are informed by reports of real cases and are grounded in medical practice reality.

In order to make best use of the case vignettes the reader should refer back to Part II to ensure that a correct interpretation of the legal terms is understood.

Case Vignette 1

Wilhelm WOLFGANG, 50, a building construction manager from Stuttgart, has suffered from multiple allergies both respiratory and dermatological, since he began working on construction projects at age 18. Other than the recurrent allergies, Wilhelm, a non-smoker, has generally been in good health.

Unfortunately his most recent routine X-ray has revealed some suspicious areas on the upper right lung. Wilhelm's specialist, Dr. Willy WEISS would like to ask a second opinion regarding the images and the case.

He has identified Prof. Alexander ARTEMIS, a world expert of pulmonary imaging in the detection of rare lung diseases, located in Greece.

Dr. WEISS wonders whether the digital X-ray images can be transferred safely and securely to Prof. ARTEMIS. A conversation with Prof. ARTEMIS reassures him on that score. In addition, Prof. ARTEMIS is quite happy to provide his analysis free of charge.

Wilhelm is hoping that Prof. ARTEMIS can provide his opinion from a distance, although he is willing to fly over, if the expenses can be reimbursed. Wilhelm thinks that two opinions give more credibility to the decisions that will follow.

The legal analysis

In this case we see at first a typical doctor-patient relationship. Below we look carefully at the case of Dr. Weiss and his patient Wilhelm and consider the legal duties incumbent upon Dr. Weiss and also those of Prof. Artemis.

The legal analysis of data protection issues starts with the identification of the processing of personal data. First we have to verify the presence of personal data. Here personal data are at stake : the X-ray images are information relating to an identified person :Mr Wolfgang. And as they relate to his health they are medical data.

In presence of personal data we have to check whether they are part of an automated or partially automated data processing or part of a filing system. Again, in this case, it is possible to say that the X-ray images are processed by automated means or that they are part of a filing system or of an electronic medical record.

Here the X-ray images are processed for and in the framework of a medical purpose.

After the identification of the data processing, we have to identify the main actors of the data processing. Usually Dr Weiss will be regarded as the data controller and Mr Wolfgang is without any doubt the data subject.

Given that the data are medical data, Dr Weiss will be subject to the special rules concerning the processing of sensitive data.

After the identification of the data processing, we have to determine its base of legitimacy. As explained, it is possible to use several bases of legitimacy i.e. the consent of the patient or the

therapeutic purpose. Here Dr. Weiss processes Wilhelm's medical data as a registered medical practitioner, and as such he is entitled to collect and process such data as it is needed for medical diagnosis and the provision of care or treatment to Wilhelm without necessarily requiring consent for the data collection and processing. In this case the medical data have to be processed by a health professional subject under national law or rules established by national competent bodies to the obligation of secrecy or by another person also subject to an equivalent obligation of secrecy.

Dr. Weiss is however under a duty to ensure that his practice and its data processing are duly notified to the relevant national supervisory authority and to inform his patients. He is also under a duty to ensure the quality of the data and the confidentiality and the security of the data processing. His patients, such as Wilhelm, have the right to access the data and rectify any mistakes that they might find.

Dr. Weiss now wishes to communicate Wilhelm's X-Ray images to a third party, Prof. Artemis. The third party in question is a medical doctor, in a European Union country and the data is being communicated for the purposes of providing medical diagnosis.

The first question to address is to know whether the communication of the X-Ray images to Prof. Artemis is compatible with and necessary for the purpose of the data processing initially conducted by Dr Weiss. The answer is evidently positive if complying with special rules i.e. medical secrecy. From a data protection viewpoint, as done in order to provide care and treatment by a medical practitioner, Wilhelm's consent to the communication would not be needed. But he should be informed about the recipients or the categories of recipients of the data, 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. In this case, the information about the communication of data to Professor Artemis seems to be mandatory when combined with ethical considerations. However, if possible and appropriate, Dr. Weiss should render the data anonymous and should not reveal the name of Wilhelm Wolfgang. Wilhelm's consent to the anonymisation would not be needed even if the anonymisation is a processing of personal data and is subject as such to data processing requirements. It should be noted, however, that anonymisation is not easy. An identification of anonymised data subjects is sometimes easier than the controller thinks. For example, reducing the name to initials will regularly be insufficient. "Real" anonymous data can be transferred without being subject to specific requirements. Again, normal ethical practice would, however, require that Dr. Weiss inform Wilhelm about his intent to seek a second opinion and to obtain Wilhelm's consent, even if the data are anonymous. In this analysis, however, we will look only at the legal rules on data handling and not at the wider ethical issues.

In the context of his duties as data controller and if anonymisation doesn't occur, Dr. Weiss is asking Prof. Artemis to process Wilhelm's data further. Dr. Weiss should ensure that Prof. Artemis and his hospital provide sufficient guarantees on technical and organisational security measures and sign a contract with him. The communication of personal data made by Dr. Weiss to Professor Artemis should be secured (for instance, by using encryption). If the transfer to Prof. Artemis's hospital is done, only Prof. Artemis should have access to Wilhelm's medical data.

Prof. Artemis will be processing the personal data on behalf of Dr. Weiss and will be therefore considered as a processor. He should therefore respect the condition of processing by a processor and must therefore act only on instructions of Dr. Weiss and must take the appropriate technical and organizational measures of protection. And again the medical data have to be

processed by a health professional subject under national law or rules established by national competent bodies to the obligation of secrecy or by another person also subject to an equivalent obligation of secrecy even at the sub-processing level.

Case Vignette 2

Dr. Caroline CARRINGTON is a general practitioner who recently arrived in a busy group practice, in Loch Harlow, Lannockshire, Scotland. Dr. Carrington replaced Dr. Charles CRAMER, when he retired in May 2006, inheriting his carefully handwritten records.

Dr. Carrington wanted to switch to digital records as quickly as possible, before multiplying her own additions to the files.

Dr. Carrington's problem on how to digitise Dr. Cramer's files seemed to find a providential answer, when she opened an envelope from SoftMicro Ltd, multinational software specialists. Inside there was a prospectus indicating that International Medical Records Coordinators (IMRC) Ltd, a division of SoftMicro, would be stopping in Loch Harlow over the summer to provide record scanning services.

Founded by Dr. , a practicing physician in the UK, IMRC had been sold to SoftMicro in 2005. IMRC's business was based on Dr Gandhi's connections between the UK and India. IMRC scans patient records in a mobile unit stationed outside British practices, sends them to IMRC offices in India for data entry to populate a data base hosted on a UK website. The website includes access by the physician to various risk calculators and alert services and is available for a very reasonable monthly fee, the equivalent of pennies per patient.

Dr. Carrington wonders whether it is safe for the files to leave her office, even though they are only being transported to the mobile truck and back. What if other colleagues need to access the files? Will her patients want to access the electronic file?

The legal analysis

Dr. Carrington processes the medical data of her patients. In some jurisdictions, like Germany, the successor does not automatically take over the right of access to documents of his predecessor. He will then need particular consent of the patients to take over the files. If this processing is purely manual, i.e., paper only, it will be covered by the data protection legislation if it forms part of a filing system or is intended to form part of a filing system. Given that the medical records must be filed in someway, this would seem to be very likely. If any automatic processing is used, then the rules of data protection will apply regardless of the nature of the processing.

The processing of personal data is carried out by Dr. Carrington for the medical care and diagnosis of her registered patients. Accordingly such processing is covered by the rules concerning medical data and does not need the explicit consent of the patients if the processing is made by a health care 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 (ex. secretary or assistant).

However, Dr. Carrington, or her group practice if the latter acts as data controller, has a duty to inform patients about the data processing and to notify the data processing to the relevant national supervisory authority. Dr. Carrington, or the practice, would also need to ensure the lawfulness of the data processing and that the quality of the data held is adequate (accurate) and that patients are informed about the data processing and have the opportunity to access and

rectify the data. Given that medical data are especially sensitive, Dr. Carrington or the group practice would also have to ensure that the data are held securely and that confidentiality is respected. As medical data have to be processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy any processing conducted by staff other than health care professionals, such as administrative staff, would have to be under a contractual or a legal duty of confidentiality which could result in termination of employment if confidentiality were broken. A policy access to the medical files should be created.

Thus we see that Dr. Carrington has a legal right to collect and process the medical data of her patients in order to provide them with medical cares. Now, however, she wishes to communicate her patients' medical files to a third party in order to scan the data and to digitalize her patients' medical records. The digitalisation of the medical files is a data processing.

The question to address here is to know whether such operation upon the patients' medical data (its digitalisation) is compatible and necessary with the initial purpose of the data processing by Dr Carrington or the practice to provide the patients' with medical cares. To solve this question it has to be reminded that creating digital records may allow her to give better care to her patients and therefore may be considered as necessary for the purposes of medical diagnosis and the provision of care or treatment.

The next question to address is how the digitalisation of her patients' medical records should occur. Here Dr Carrington would like to benefit from the IMRC services in digitalizing medical records. The intervention of IMRC in order to digitalize the medical records on her behalf could easily be justified.

A first problem could result from the transport of the medical files to the mobile unit outside the practice. It is not evident to state the compliance and lawfulness of this procedure. If the transport of the files in the mobile truck is unsecured, Dr. Carrington will be liable for this as well as IMRC. If this procedure is considered as normal procedure Dr Carrington would need to ensure in any case that IMRC have the medical records for a minimal amount of time and that the transport and the digitalisation are realized 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 (otherwise the digitalisation would require another base of legitimacy i.e. the explicit consent of the patients).

As IMRC will process the data on behalf of Dr. Carrington and will therefore be considered as a processor, Dr. Gandhi should ensure that IMRC provide sufficient guarantees on technical and organisational security measures and that they sign a contract with Dr. Carrington. She would also have to ensure that the contract to digitise the records included a clause stating that confidentiality and a high level of security must be maintained for patient records.

On the other hand Dr Carrington or the practice should inform the patients about the digitalisation in order to ensure a fair data processing due to the intervention of a third party in the process that was not predictable for the patient.

However, IMRC intends to do more than simply digitise the records. Once scanned, the digitalized medical files will be sent to India (thus outside the European Union) in order to populate a searchable database of the medical records located in UK. The transfer of data to India could only be permitted if India ensures an adequate level of protection. Today India does not seem to ensure such level of protection. But the transfer could be done with the

unambiguous consent from the patient to the proposed transfer or with a contract signed between Dr. Carrington and the recipient of the personal data imposing to the latter the conditions of the data processing, if complying with medical secrecy rules. Regarding this Dr Carrington should use the standard contractual clauses from the European Commission to ensure an adequate level of protection. Regarding the sub-processing in India the recipients of the communication have to be subject to confidentiality rules equivalent to those incumbent to health care professionals.

Again to ensure a fair data processing Dr Carrington or the practice should inform the patients that the digitalized medical records have been sent in India to be encoded in a database located in the UK.

Finally there could be a problem with the hosting of the medical records on a website in the UK (outside the offices of Dr Carrington and of the practice). Indeed the provision of care does not require per se the availability of the patients' medical files online through a website. Regarding this point the legitimacy of the processing of the medical files could require at least the consent of the patients after being completely informed about the hosting. But even with the patients' consent it is not sure that the hosting of the medical files on a website should be permitted. With respect to the latter it could be useful to check the lawfulness of such practice and to consider the special risks created by this project. In this extent the project should be subject to a prior checking accordingly to Article 20 of the directive. The security of the website should at least be strongly audited on a regular base.

Nevertheless the patients should also be informed about their right of access to their medical data even during the digitalisation and the encoding processes and the continuity of care have to be ensured during all the process.

Case Vignette 3

Sophie and Sandrine SANDEAU are identical twins with a congenital cardiac disorder that led to the implantation of their first pacemakers at age 40.

Sophie is a biologist with the French Medical Research Institute in Paris. Sandrine is a mystery novelist, well known in the Bordeaux area for her vineyard murder series. Both sisters support the work of the French Association of Congenital Cardiac Disorders.

Six years after the implantation of their first pacemakers, Prof. Serge SIMON, the head cardiac surgeon at a state-of-the-art French hospital, performed an innovative surgical procedure on the two sisters at six-month intervals, first Sophie and then Sandrine.

The sisters' case created great academic interest in France, and the surgeon, who knew Sophie professionally, asked her if she would authorize the hospital to use the data of her case in a publication. Her response was positive. Sandrine was not made aware of Sophie's authorization.

Serge presented Sophie case at a special staff meeting, which was projected by simultaneous videoconference to the Senegalese medical school in Dakar. Prof. Simon did not consider that this communication was a publication, since the videoconference recording never left the files of the establishments.

Prof. Simon's colleague at the hospital, Sasha SUREAU, helps the Cardiac Surgery Department increase its research financing by selling cardiac images to an international textbook publisher based in New York and London. Sasha SUREAU sells images taken during the recent surgical interventions on both of the sisters.

The Sandeau sisters are not aware of the hospital-textbook publisher relationship. But Sophie's son, Steven SANDEAU, who is studying medicine, came across a case which he thought was remarkably similar to that of his aunt Sandrine. He did not imagine that it was in fact Sandrine, given that the textbook was not published in France.

Sophie and Sandrine have just read that the French Association of Congenital Cardiac Disorders would like to accept the Dupont Medical Informatics Company offer to host an open electronic e-mailing list for discussion of cardiac topics. Dupont already hosts such a list in French on a Canadian server, as well as a list in Spanish on an Argentine server. Sophie will probably sign up for it and is wondering what legislation prevails given the multi-country locations of the servers.

The legal analysis

We will now consider the various activities and roles sin the case of the Sandeau twins from a data protection viewpoint.

As usual the first step consists to check the presence of personal data. The data at stake are information relative to the cardiac disorders of the Sandeau sisters and their medical treatments. These information are gathered in their respective medical records. These information are personal data and to be more accurate they are medical data.

To fall under the scope of data protection regulations these medical data have to be processed by automated means or to be part or intended to be part of a filing system.

We may assume that the medical records of the Sandeau sisters are in electronic format or at least constitutive of a medical file, both situations inducing the application of data protection rules.

The base of legitimacy of this data processing lays in the purpose of providing both sisters with medical care.

The controller has a duty to ensure the quality of the data i.e. that they are adequate and necessary for the therapeutic purpose and correct.

The hospital must ensure that the data are processed fairly and lawfully and must not reuse the medical data in a way incompatible with the initial data processing purpose (support the provision of health cares).

The controller should provide Sophie, the data subject, with the relevant information about the processing and should allow her to exercise her access right.

The security and the confidentiality of the data processing have to be ensured. The latter implies to prevent inappropriate access to the medical data (creation of an access policy to medical files). Therefore a control should occur when someone is willing to use the medical data for publication, staff meeting, video projection and sale of medical images.

Finally the data processing has to be notified to the national supervisory authority.

Publication

The first issue to address is the use of information from Sophie's medical record for a publication.

If the data are anonymised there won't be any problem from the data protection perspective for using them in a publication. But special rules could exist in national law (i.e. medical secrecy rules) regarding the conditions use information from clinical practices in a publication. And we have to be sure of the data anonymisation. It has to be impossible to identify the data subjects using reasonable means. In the present case the medical story of both sisters have aroused a great interest in academic circles in France. As the surgery was quite innovative it is not sure that the anonymity of both sisters could be ensured considering also the notoriety of Sandrine as a mystery novelist and the professional notoriety of Sophie as a biologist with the French Medical Research Institute in Paris. This point has to be checked very precisely.

If the medical data can not be anonymised the question to solve is to know whether the use of personal data from the medical records for publication is compatible and necessary regarding the initial purpose of the data processing i.e. providing Sophie with good health cares. The answer is negative and we will assume that this further use of her medical record is not compatible with the initial purpose of the processing of Sophie medical record. Therefore Professor Simon has to find another base to legitimate the use of the medical records for publication and to respect the special rules applicable to medical data such as those relative to medical secrecy. From a data protection viewpoint he could rely on the explicit and hence informed consent given by Sophie. The question to know if he should have also the explicit consent of Sandrine for legitimating purpose when using the medical file of her sister Sophie is controversial. The 29 Working Group

party states in an opinion that this question should be treated case by case in deciding how to address possible conflicts between the interests of the data subjects and those of their biological family. The need of consent of Sophie's sister is therefore not excluded, nor is it categorically called for in the EU-level legislation, although some specific regulations in Member States may have dealt with this particular issue. But the answer should be positive if Sandrine could be identified through the publication. Indeed in the latter case the publication would reveal sensible data concerning Sandrine in a way incompatible with the initial purpose of her medical data and without any base of legitimacy and presumably in violation of medical secrecy.

In any case if the publication is compatible or presents a base of legitimacy the data must be adequate and relevant and cannot be excessive. The picture of the heart, or the implantation of the pacemaker should not include Sophie's face or any elements that may link to her, unless it is necessary or unavoidable.

Staff meeting and Video projection

The second issue to deal with is the further use of Sophie medical record at a special staff meeting that was projected simultaneously to the Senegalese medical school in Dakar.

If the images allow anyone to identify directly or indirectly Sophie (or her sister), those images may be legally classified as personal data within the terms of data protection legislation. The first advice is to anonymise the personal data used during the meeting. And if the images are completely anonymous their video projection with the Senegalese medical school in Dakar will not be subjected to data protection rules. Note, however, that it will not be simple to decide if the images are legally classified as anonymous for both sisters : if Sophie's heart condition is sufficiently rare, any publication of an image of case history could be classified as person-identifiable even if all usual identifiers (name, date of birth, address, etc.) have been stripped from the data. We have also to check if her sister Sandrine could not be identified directly or indirectly.

If it is not possible to anonymise the data we could consider that the use of her medical record at a special staff meeting is compatible with the initial purpose at least for peer-reviewed concern and improvement of the healthcare quality. Naturally the data processing will occur under the responsibility of a health professional. Sophie should be informed about the use of her medical data at the staff meeting i.e. to ensure a fair data processing.

The data must be adequate and relevant and cannot be excessive. The picture of the heart, or the implantation of the pacemaker should not include Sophie's face or any elements that may link to her, unless, it is necessary or unavoidable.

Regarding the simultaneous projection by videoconference with the Senegalese medical school in Dakar we have first to check if it constitutes a data processing. The answer is positive in theory but could raise practical problems in the implementation of some data protection rules i.e. regarding the access right if the images are not recorded. But in this case the video projection is recorded by the hospital. The video projection constitutes hence an automated data processing inducing the application of data protection rules i.e. its notification to the supervisory authority.

Then the next question concerns the compatibility of this video projection with the initial purpose of the processing of personal data from Sophie's medical record. A first view this video projection does not appear compatible. Hence Professor Simon has no base of legitimacy to perform such video projection. He could ask for the explicit consent of Sophie after given her enough information about the video projection. Therefore, Sophie would have to have been

informed that the images would be used in an educational videoconference i.e. to ensure a fair data processing.

Next if he could use such base of legitimacy he still has to check if the video projection constitutes a transfer of personal data and a transfer of personal data outside Europe. It is not sure that the video projection induces a transfer of personal data. But if the Senegalese medical school records the video projection there will be a transfer of personal data outside Europe. And as Senegal does not ensure at the moment an adequate level of protection the transfer is not allowed except for having the (informed) consent of Sophie or a contract with the contractual clauses accepted by the European Commission. And again the rules relative to medical secrecy have to be met. The controller would also have had to ensure that that specific purpose was duly notified to the relevant national supervisory authority and the security of the data transfer.

In any case the data must be adequate and relevant and cannot be excessive. The picture of the heart, or the implantation of the pacemaker should not include Sophie's face or any elements that may link to her, unless, it is necessary or unavoidable.

Sale of medical images

The sale of the images taken during the surgery on both sisters Sandeau by Sasha Sureau, Professor Simon's colleague, is a communication of their personal data from their medical records.

The first question to address is to know whether the images allow the identification of the sisters using reasonable means. Presently it could be stated that their identification is reasonably conceivable. Indeed Sophie's son, Steven Sandeau, a student in medicine, came across a case which he thought was remarkably similar to that of his aunt Sandrine.

In presence of personal data we have to check if their communication could be viewed as compatible with the initial data processing purpose. The answer is clearly negative. This could also constitute a breach of the medical secrecy.

From a data protection perspective, the sale of these images is new data processing and thus requires at least the informed consent of both sisters. Mr Sureau still should verify whether the applicable national law allows the sale of medical images even to fund medical research. This question raises an important ethical question.

In any case the data should have to be adequate and relevant and cannot be excessive. The picture of the heart, or the implantation of the pacemaker should not include Sophie's face or any elements that may link to her, unless, it is necessary or unavoidable.

Discussion forum through e-mailing list

The French Association of Congenital Disorders wishes to set up an open e-mailing list. The Dupont Medical Informatics Company offers the Association to host an open electronic e-mailing list for discussion of cardiac topics. Dupont already hosts such a list on a Canadian server as well as a list on an Argentine server. Sophie and Sandrine would like to participate to this forum.

The creation and the functioning of the forum will require the processing of personal data by automated means. Hence data protection rules apply. The forum will imply the processing of

personal data concerning all its members i.e. both sisters to create the e-mailing list. Then there will be processing of personal data when forwarding e-mails to the members of the forum and maybe the storage of all the distributed emails on a server for future members. It has to be reminded that cookies are data processing and have to be treated consequently.

The operations performed upon these personal data have to be identified as well as their purposes. We have already identified the creation and the functioning of the forum. The base of legitimacy of these processing should rely in this case on the explicit consent of the data subjects (the members of the e-mailing lists).

The fairness of the data processing requires its notification to the national supervisory authority and the adequate information of the forum members on the data processing including information about the roles of Dupont Medical Informatics as processor of the Association.

The data processing should also be lawful and meet the special rules that might exist concerning this kind of forum (code of conduct, etc.).

The quality of the data implies the adequacy, the relevance and the updating of the processed data especially regarding the updating of the electronic addresses and of the member list. As personal data have to be stored for a limited period of time, when a user decides to unsubscribe from the e-mailing list, his or her e-mail address and other personal data should be erased. In the same time the members of the forum should have access to the processed data concerning their person (i.e. email address and identification elements).

The data controller (the French Association) has to ensure the compliance with the data protection rules applicable to the forum and especially to ensure the confidentiality and the security of the data processing. Regarding this we should focus on the security measures to prevent unauthorized or inappropriate access or diffusion of e-mail considering their informational content that could be very sensitive. An example of measure could be to avoid the appearance of the members' name to each other.

A mention has to be done regarding the intervention of Dupont Medical Informatics when hosting the emailing list. Here Dupont Medical Informatics acts as a processor of the French Association, the data controller. The French Association must therefore respect the conditions for the transfer of personal data to a processor, which include ensuring that the processor provides sufficient guarantees on technical and organisational security measures and to sign a contract with it. Subscribers should be informed adequately about the intervention of this company. This results from the data subjects' information right that participates in the same time at the data processing fairness.

Finally, we should check if there are transfers of personal data outside Europe in the forum. Here we may note that Argentina and Canada enjoy from a favourable legal regime for the transfer of personal data from Europe since they have been acknowledged by the European Commission as ensuring an adequate level of protection. Nevertheless, the conditions of transfer have to be respected (for instance, the transfer to the Canadian server benefits from the favourable regime whether the Dupont Medical Informatics Company is subject to the Canadian Personal Information Protection and Electronic Documents Act (PIPED Act)).

Case Vignette 4

Bert BEMELMANS, a 38-year old Belgian, was born with a rare disease, Nafram Syndrome, which he inherited from his father, Bert Sr. As the son of a Nafram Syndrome patient, Bert Jr. was diagnosed early on. Barring the limitation on strenuous athletic activity incurred by Nafram Syndrome, Bert Jr. enjoys a normal life.

Bert's mother's career as an economist took the family from Belgium to Bristol in the UK in 1986. But Bert Jr. returned to Belgium to complete his masters' degree and settled down in Liège with a family of his own, while his parents remained in Bristol. Bert Sr. passed away in 2004 in the UK.

Bert Jr., who devotes much of his free time to bird watching, makes little private use of the family's computer. He is thankful that his daughter Beverly, 16, searches the Internet for him, whenever she can snatch the family computer away from her videogame enthusiast brother.

Beverly signed up for several medically related e-mailing lists, including one on Nafram Syndrome. She created a special e-mail address for this purpose, under a shortened version of the family surname "Elmans". Generally, participants' e-mails are not visible on the medical e-mail lists. However, Beverly was surprised to see one message pass by on the Nafram list, clearly identified as coming from her father's general practitioner (GP). She doubted that there were any other Nafram Syndrome patients besides her dad in his clientele and is worried that people would know that the physician was requesting information that could be useful to her father.

Beverly is also concerned that the confidentiality of her deceased grandfather's medical file is not guaranteed under British law, and that the problem is aggravated by the fact that father and son bear the same name.

The Bemelmans family is interested in following the activities of the Belgium-based European Association of Nafram Syndrome Patients. Beverly recently received a query from the European Association who was looking to survey patients about the disease's impact on their professional life. Beverly showed the survey to her father who agreed to participate; the organizers ensured them that the information would remain confidential. However, Beverly read that the national Belgian Nafram Association would like to share in the results of the study as well, and she was wondering if her father's physician may be able to identify Bert's answers.

After a cursory review, Beverly filled in an online form indicating that she had her father's permission to collect his interview answers. She indicated that she was born in 1985 rather than 1990, just to be on the safe side… but she dutifully transcribed her father's answers, rather than imagining what they would be.

The legal analysis

The case above poses a number of legal questions concerning the collection and processing of data concerning Bert Bemelmans and his father. The analysis below picks out the most important legal issues in order to illustrate the ways in which the data protection legislation works in practice.

The first step consists to identify automated data processing or data files at stake in the various situations described in the case.

Three situations emerge in this perspective : the emailing list of the European Association of Nafram Syndrome Patients, the protection of Beverly grandfather's medical record and the survey on the disease's impact on patients' professional life.

The e-mailing list of the EANSP

The creation and the use of a mailing list require in some extent the processing of personal data from the subscribers. The participation of the subscribers to the mailing list provides information about their health as the association brings together persons suffering from Nafram disease, which is very specific. Therefore we could say that the information used for the creation and the use of the mailing list could provide information about the subscriber's health. Hence we are in presence of medical data and they are processed by automated means, inducing the application of data protection rules.

The controller of the list as well as the purposes of the list must be identified. The EANSP will be the data controller. But the EANSP is not a medical practitioner with a right under the data protection legislation to collect sensitive data, nor would it seem that the data are being collected for the purpose of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services. Accordingly, the controller of the mailing list will have to obtain the explicit consent of the data subjects to the inclusion of the e-mail address. In this case the mailing list works on a voluntary base. Therefore the base of legitimacy of the mailing list will rely on the explicit (and informed) consent of the subscribers. Here Beverly has just given her father's e-mail address with his authorization. But was Beverly legally entitled to represent her father in this case? The answer could be controversial. It has to be solved regarding the national rules concerning the persons' legal or conventional representation.

In order for the e-mailing list to be operated legally, the controller of the list would have had to comply with a number of other rules and would have to ensure that he or she had notified the processing to the relevant national supervisory authority.

The e-mailing list controller must process the data fairly and lawfully and must not reuse the e-mail addresses for purposes other than those accepted by the users. Notably, the list controller could not use the database to make direct marketing if this purpose was not initially accepted by the list subscribers. The members of the list have to be duly informed about the data processing to ensure i.e. its fairness and its legitimacy since it is based upon the explicit (and informed) consent of the subscribers.

The controller must also take every reasonable step to ensure that the data are accurate. For instance, the controller must allow the users to modify their personal data (their email address by example); accordingly they must know what data are held about them. The data collected must be adequate and relevant and cannot be excessive for the stated purpose. Generally, in order to manage an e-mailing list providing medical information, the controller would not need to know who suffers from a disease, for how much time and which medication the list subscriber uses. It would therefore be hard for the data controller to justify the collection of such data from Beverly or Bert.

Personal data should be stored for a limited period of time. When a user decides to unsubscribe from the e-mailing list, his or her e-mail address and other personal data should be erased.

The controller should provide the users with the relevant information about the nature and type of data processing and should allow them to exercise their access and rectification rights.

The controller has the obligation to ensure the security (against loss, destruction, distortion, etc.) and the confidentiality of the personal data processed (i.e. against illegal disclosure of the subscriber list).

The controller should also ensure that the appropriate technical or organisational measures to achieve this purpose have been taken. For example, the controller should create a contractual duty of confidentiality for his employees, in order to avoid any disclosure of information to third persons. This duty would normally have to be formulated such that a breach of confidentiality would be a cause for summary dismissal (i.e., without notice). It is forbidden to communicate to third parties the name of the users of this e-mailing list (for example, informing the press that a celebrity is a subscriber). Any electronic communication of personal data should be encrypted. In this case, therefore, the data controller may be guilty of a breach of confidentiality if the content of the list and the naming of Bert's GP is such that a reasonable person could deduce Bert's identity from the discussions on the list.

In this case vignette we have looked at an e-mail subscription list to which users are knowingly subscribing. It might occur, however, that a drug manufacturer or alternative health care practitioners operate a simple website which just provides information about their products or services. If the provider of such a health website is processing personal data of the Internet users (by the use of cookies, for instance), or of some patients (whose medical information are part of the content of the website), they would also be required to respect the data protection legislation (see above).

The protection of Beverly grandfather's medical record

Beverly has some concerns about the protection of her grandfather's medical records. The application of data protection rules to data relative to dead persons is controversial. But their protection could be guaranteed by the rules relative to medical secrecy. Regarding this point the European Commission on Human Rights has considered in 1988 that the protection of the medical record of a deceased person is a legitimate interest.

The survey on the disease's impact on patients' professional life

In this case vignette, the European Association of Nafram Syndrome Patients intends to undertake a patient survey. This brings with it a number of legal conditions for the Association.

The first advice is to conduct an anonymous survey. Then data protection rules won't apply. Unfortunately it could be difficult to reach this objective.

It is more reasonable to accept that there will be personal data (medical data) at stake due to the simple fact that the survey implies the collection of Bert's medical data and that they will be processed by automated means as the answers will be collected through an online form. Hence data protection rules apply.

In this data processing the EANSP will act as data controller. The purposes of the data processing will have to be precisely identified implying to explain the goal of the survey (why and for which results are they conducting such survey?).

The EANSP will need the explicit (and informed) consent of the participants to legitimate the collection of their answers, which might be regarded as medical data. The explicit consent will be necessary since the processing is not made for purpose of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services. As Beverly is a minor could she subscribe on the name of her father, even if he accepted to it? The question is controversial and has to be solved regarding national rules concerning legal and conventional representation.

The quality principle imposes that the EANSP does collect only the necessary data to realise the purpose assigned to the survey.

The EANSP will have to inform adequately the data subjects about the data processing.

The data subjects will have the right to access their personal data and should be entitled to rectify error in their answers i.e. in case of wrong encoding or error in the manipulation of the survey form.

The EANSP will have to ensure the confidentiality and the security of the data processing. The EANSP has to ensure the security of the collection of medical data through the telematic network and their security on the server against i.e. inappropriate access, disclosure, alteration or diffusion.

The EANSP will have to notify the data processing to the national supervisory authority and to inform the patients about the data processing to ensure its fairness and its legitimacy.

Finally the Belgian Nafram Association wishes to use the results of the survey. Is EANSP entitled to transfer the information obtained from the survey to this other association?

If the data are rendered anonymous, data protection rules won't apply to their transfer. The question will focus on the way to anonymise the data.

If the data cannot be anonymised the question to solve will be to know if the communication of these data is included or compatible with the initial purpose of the data processing. We could note that the information provided to the data subjects in the initial data processing never announced such transfer. And regarding the very sensitive nature of the data at stake the answer regarding the compatibility should be negative. Could the coding of the data result in the compatibility of the transfer? Normally in this case as coded data remain personal data (here medical data) the transfer could only occur with the explicit (and informed) consent of Bert Junior (except for the possibility of another base of legitimacy). Whether we consider that the further processing pursues scientific, historical or statistical purposes the transfer will be compatible if the national safeguards are met

If the European Association communicates personal data to the Belgian Nafram Association, the latter will also be subject to the data protection legislation, as the latter will conduct a data processing for which it will act as a data controller.

The BNA will have to identify precisely the purposes of the data processing that it wishes to conduct and to find a base of legitimacy. If the data processing purpose is not scientific, historical or statistical, the BNA should ask for the explicit (and informed) consent of the data subject, Bert

Junior, safe for another base of legitimacy in national law. If consent is required, as data are coded, the consent will have to be asked by the first data controller.

The BNA will process only the necessary data according to the quality principle.

The data processing will have to be fair. In consequence the BNA will have to notify the data processing to the national supervisory authority and will have to inform adequately the data subjects about the data processing. The duty of information could not apply if the initial information made by the European Nafram Association covers the processing projected by the Belgian Nafram Association. Moreover, since the collection is indirect, the duty of information could be exempted if the processing of the Belgian Nafram Association is made for statistical purposes or scientific research and if the provision of such information is impossible or would involve a disproportionate effort. The Association would also need to ensure that the data were held securely using state-of-the-art technology appropriate for securing the confidentiality of this type of data.

The Belgian Nafram Association should allow the data subjects to exercise their access and rectification rights.

PART IV: LEGAL SOURCES

Clicking on the links will take you directly to web resources showing the legislation in full (in English).

Data protection is governed by a certain number of international **legally binding** texts.

- Directive 95/46/CE of the European Parliament and of the Council of 25 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data
- Directive 2002/58/CE of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
- Directive 2006/24/CE of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
- Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community, institutions and bodies and on the free movement of such data
- Article 8 of the European Convention on Human Rights
- Articles 7 and 8 of the Charter of fundamental rights of the European Union
- The Convention n°108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted on 28 January 1981
- Convention n°164 for the protection of Human Rights and dignity of the human being with regard to the application of biology and medicine: Convention on Human Rights and Biomedicine and its Additional Protocols

Some recommendations are also made to the countries that are **not legally binding but are policy guidelines** on specific fields of data protection:

- Recommendation (97) 5 of the Committee of Ministers to Member States on the protection of medical data, adopted on 13 Feb. 1997
- Recommendation (83) 10 of the Committee of Ministers on the protection of personal data used for scientific research and statistics, adopted on 23 September 1983Recommendation (97) 18 of the Committee of ministers of Members States concerning the protection of personal data collected and processed for statistical purposes, adopted on 30 September 1997
- Recommendation (99) 5 of the Committee of ministers of Members States for the protection of privacy on the Internet, adopted on 23 February 1999
- Communication 2004 (356) from the Commission to the Council, the European Parliament, the European economic and social committee and the committee of the regions "eHealth - making healthcare better for European citizens: an action plan for a European eHealth area"
- Some opinions or recommendations made by the Data Protection Working Party
- Opinion n° 13 (1999) of the European Group on Ethics in Science and New Technologies on Ethical issues of healthcare in the information society