

**RECOMMENDATION 2/2004 ISSUED BY THE DATA PROTECTION AGENCY OF THE MADRID
REGIONAL GOVERNMENT ON THE SAFEKEEPING, FILING AND SAFETY OF PERSONAL DATA
CONTAINED IN NON COMPUTERIZED MEDICAL RECORDS**

Act 41/2002 of 14 November regulating the patient's independence and the rights and obligations as regards clinical information and documentation, in response to the European Council Convention on the protection of human rights and the dignity of human beings with regard to biology and medicine applications (Convention on Human Rights and Biomedicine), signed on 4 April 1997 and which became effective in the Kingdom of Spain on 1 January 2000, and in response to Recommendation of 13 February 1997 on the Protection of Medical Data issued by the European Council, establishes as its first basic principle that the dignity of every person and the respect for their free will and privacy shall guide all activities aimed at obtaining, using, filing, safekeeping and transmitting clinical information and documentation.

This regulation came into force in May 2003 and from that moment became the rule of reference in Spain, completing the provisions of the General Health Act and defining and regulating medical records, without prejudice to the possibility that each Regional Government with jurisdiction over health matters may complete the aforementioned legal text. As regards the Madrid Autonomous Region and in order to complete this legal framework, the Department of Health and Consumer Affairs has set up a Group of Experts in Clinical Information and Documentation which is reviewing different aspects to be incorporated into this new regional Act, such as access to clinical documentation, professional use of medical records, access by patients and other organisations, and intrahospital and extrahospital communication.

However, at present Act 12/2001 of 21 December applies. This Act on the Regulation of the Health System in the Madrid Autonomous Region establishes that guidance of the citizens as human beings, their independence, and their right to privacy and protection of personal data are the basic principles governing the organisation and operation of the Health System.

In accordance with Chapter V of Act 41/2002 of 14 November, the main purpose of medical records is to facilitate the provision of health care, as an instrument aimed basically at ensuring the provision of adequate care to the patient, and shall include the set of documents related to health care processes and the information considered vital for obtaining an accurate and up-to-date picture of the patient's state of health. Moreover, this legal text reinforces, stresses and insists on the recognition of the right of the individuals to demand that the confidentiality of the data related to their health be respected, and to deny access to those data without their prior consent as set forth by law, and establishes that the dignity of every person and the respect for their free will and privacy shall guide all the activities aimed at obtaining, using, filing, safekeeping and transmitting clinical documentation.

But clinical records are also the source of information required for many other purposes for which they may be useful, including for judicial, epidemiological, public health, research or educational reasons, all of them legitimate and related to fundamental activities carried out by the Health System, and based on which the aforementioned act also regulates their content, filing, processing and use.

Thus, it must be understood that the personal data contained in all documents and information which are a part of medical records, without prejudice to the aforementioned legal provisions, are protected specifically by Organic Act 15/1999 of 13 December on the Protection of Personal Data, which in Article 7 defines this information as specially protected data, since they are records on the health of the citizens, and establishes a particularly strict set of rules for their acquisition, safekeeping and possible transfer.

Consequently, health-related personal data which are a part of medical records shall be incorporated into a structured computerized or manual file which will include the medical records of each health care centre, the processing and use of which fall under the scope of Organic Act 15/1999 of 13 December on the Protection of Personal Data, in accordance with the provisions of Article 2 of this legal text, which sets forth that this Act shall apply to personal data recorded on physical media which enable their processing, and to any subsequent use of this data by the public and private sectors.

Based on this premise, that is to say, the existence of files structured in either a manual or computerized fashion which contain all the medical records of each health care centre, and although

the trend is for medical records to be computerized, since presumably through this computerization greater safety will be made possible with the application of Royal Decree 994/1999 of 11 June approving the Safety Regulations for automated files containing personal data, at present, however, many health care centres both in the Madrid Autonomous Region and in other Communities lack automated procedures for fully managing medical records, and most of them still use manual processing procedures for managing this information. This circumstance makes it necessary to implement protocols for ensuring that the confidentiality of health-related data is not violated by unauthorised persons; for preventing this information and documentation from being transferred to third parties without proper legal guarantees and precautions; and for establishing safekeeping and filing measures. These will be protocols aimed at protecting the privacy of patients, bearing in mind also that the aforementioned Safety Regulations are designed for computerized files and processing.

Act 8/2001 of 13 July on the Protection of Personal Data in the Madrid Autonomous Region establishes that the Data Protection Agency of the Madrid Regional Government shall be responsible for controlling personal data files created or managed, among others, by the institutions of the Madrid Autonomous Region and by the organizations, bodies and other agencies of its Public Administration (Article 2), and therefore all health care centres which are accountable to the IMSALUD and the Department of Health and Consumer Affairs of the Madrid Regional Government fall under the scope of this Act.

The Data Protection Agency of the Madrid Regional Government, bearing in mind that most files and data processing procedures related to the medical records of the aforementioned health care centres were in place prior to the coming into force of Organic Act 15/1999 of 13 December, and in accordance with the function it has been assigned under Article 15 d) of Act 8/2001 of 13 July on the Protection of Personal Data in the Madrid Autonomous Region, considers advisable to issue a number of recommendations on measures for safekeeping and filing non computerized medical records, so that from the point of view of data protection they may serve as a guide and reference for the public health centres and institutions of the Madrid Autonomous Region, taking into account both the special characteristics of the manual personal data files and the fact that Organic Act 15/1999 of 13 December establishes in its First Additional provision a period of twelve years, from 24 October 1995, for non-automated files and data processing procedures to be adapted to the aforementioned Organic Act, without prejudice to the exercise of the rights of access, correction and cancellation by the affected parties.

This recommendation is not regulatory in nature, but rather a programmatic document, insofar as it may be used as a reference to be taken into account by the public authorities in health-related matters in the Madrid Autonomous Region. Its sole purpose is to attempt to clarify those questions which, from the point of view of data protection, may arise in connection with the safekeeping and filing of personal information contained in non-computerized medical records in the various health care centres of the Madrid Autonomous Region.

Consequently, and by exercising the powers conferred to it by law, the Data Protection Agency of the Madrid Regional Government issues the following recommendations:

ONE. Filing and safekeeping of the medical records file

Who is responsible for the medical records file

According to the definitions that both Organic Act 15/1999 of 13 December on the Protection of Personal Data (hereinafter the "LOPD") and Act 8/2001 of 13 July on the Protection of Personal Data in the Madrid Autonomous Region (hereinafter the "LPDCM") set forth regarding the party responsible for the file, this party decides on the purpose, contents and use of the processed data, and therefore the filing and management of the medical records file shall be, in principle, the responsibility of the management of the health care centre, without prejudice, as set forth in Act 41/2002 of 14 November, to the fact that in those centres with hospitalized patients or which look after a sufficient number of patients under any form of health care, management and safekeeping of the file may be entrusted to an Admission and Clinical Documentation Unit (hereinafter the "UNADC") which must be set up in each of the centres where a medical records file exists.

However, under the terms provided for by the regional legislation and as stipulated by the Department

of Health responsible for organizing the public health care system of the Madrid Autonomous Region, it would be advisable that whenever possible equivalent services in charge of filing and safekeeping medical records be created in those health care centres which do not fit into the previous paragraph.

Filing criteria

The basic filing criteria are contained in Act 41/2002 of 14 November regulating the patient's independence and the rights and obligations as regards clinical information and documentation (hereinafter "Act 41/2002"), which establishes that each health centre shall file the medical records of its patients, whatever the medium (paper, audiovisual, computerized, etc.), in such a way so as to guarantee their safety, proper conservation and retrieval of the information, and to make possible the exercise of the rights recognized to the interested party.

In addition, each medical record must be managed according to criteria of unity and integration at each health care centre as a minimum, in order for the physicians to have better and more convenient access to the data of a given patient during each health care process. Maximum possible integration of medical records shall be promoted, and a maximum of one file shall exist at each centre.

TWO. Safety of the medical records file

Safety document

All safety measures to be implemented at each health care centre in connection with the safekeeping and access to the medical records file must ensure the confidentiality of the data held and prevent unauthorized access, by controlling who is using the medical record from the time it leaves the file until it is returned. These measures must necessarily be documented in writing, and each centre shall be responsible for preparing this document and making sure that all the staff who may be involved in the management, handling or use of medical records are aware of its contents.

Staff obligations

When defining the obligations of the staff at each centre, a distinction needs to be made between the health care professionals who will look after the patient and the administration and management personnel. Generally speaking, both categories of staff are required to keep the confidentiality of the information, an obligation which is established both generically and with regard to personal data in Article 10 of the LOPD and in Article 11 of the LPDCM.

Health care professionals who diagnose or treat patients have full access to their medical records, as an essential instrument for providing adequate care.

Administration and management personnel in health care centres and institutions may only access the data contained in the medical records which are related to their own functions, for instance, admission of patients, prior appointments, bookkeeping and budgetary functions, etc.

However, the Madrid Regional Government shall establish by law the adaptation and differentiation procedure for accessing medical records.

List of authorized staff and filing criteria

A detailed list with all the staff who may access the medical records should exist at the UNADC or equivalent service in charge of managing the medical records file. This list may be prepared based on names or professional profiles, and whenever possible a clear distinction should be made between health care professionals and administrative staff. Based on this list, the UNADC or equivalent service shall authorize or deny access to the documents contained in the medical records.

For this purpose, it is advisable to file all clinical documentation contained in the medical records (which is clearly detailed in Article 15 of Act 41/2004) separately from all the administrative documentation which, although not a part of the medical records, may be generated as a result of the management of the medical records, such as admission records, prior appointment records, bookkeeping documents, invoices, financial costs of tests, etc.

Controlling physical access to the file

Only the staff assigned to the UNADC or equivalent service shall have access to the premises where the Unit is located, and for this purpose all required control measures must be put in place. These control measures must provide for possible emergency situations of an exceptional nature, where all required means should be used to avoid endangering life and property, including the possibility of granting access to people unrelated to these premises (fire brigade, emergency services, police, etc.). Moreover, cleaning and maintenance staff who generally have access to these premises should only have access during working hours when the personnel of the UNADC or equivalent service are present.

Likewise, all required safety means must be available at the premises to prevent any risk that may arise as a result of accidental or intentional incidents, such as fire, water leaks, etc. For this purpose, special equipment must be installed, including fire detectors, duly indicated fire extinguishers, fireproof cabinets for filing the documents, etc.

Management of the documents included in the medical records

For this purpose, it would be advisable to make a distinction between two stages in the lifecycle of the medical records. The first one would be when the medical records are active, and in this respect the law stipulates that they should be kept during a sufficient period of time in order to provide adequate health care to the patient in each case, at least for five years from the date when the patient is discharged. The second stage would be when the aforementioned period has not elapsed and the medical records become passive, but nevertheless need to be kept for judicial purposes in accordance with the current legislation, or when epidemiological or research reasons or other causes related to the organization and operation of the National Health System exist.

During the first stage, medical records should have a unique ID code per centre and contain sufficient information to identify each patient clearly and prevent errors.

During the second stage, when the medical records become passive, an attempt should be made to file them by separating the ID data from the clinical documents.

Identification of staff external to the UNADC or equivalent service who access the medical records and access log

When any of the authorized staff requests access to the data contained in a medical record, the UNADC or equivalent service must confirm that they are authorized and are included in the list indicated in point 3 of this Recommendation, and must also verify the data to which they have access, and shall provide access and deliver the requested documentation. For this purpose it will necessary to keep a log showing the medical records going in and out, together with the date of the medical record, the access date, the recipient and the return date.

THREE. Preservation, purging and transfer of the data contained in the medical records

Preservation

Safekeeping by the centres

The health care centres and institutions are under the obligation to keep the clinical documentation under conditions which ensure their proper maintenance and safety, although not necessarily on their original medium, in order to provide adequate care to the patient during the applicable time period in each case, and at least for five years from the date when the patient is discharged. For this purpose, the Madrid Regional Government may regulate and establish by law, as other Autonomous Communities have done, a longer preservation period.

The clinical documentation shall also be kept for judicial purposes in accordance with the current legislation. Moreover, it must be kept when epidemiological or research reasons or other causes related to the organization and operation of the National Health System exist. In this latter case, its

processing must be effected in such a way so as to avoid whenever possible the identification of the affected individuals.

As indicated in point 5 of this Recommendation, a distinction may be made within the file between those medical records corresponding to an active episode which has not yet concluded and those which constitute the passive file and thus correspond to concluded episodes. The provisions set forth in this Recommendation shall apply to any of these two cases.

Safekeeping by third parties

Access to data by third parties is regulated by Article 12 of Organic Act 15/1999 of 13 December on the Protection of Personal Data as a possibility of accessing such information when such access is required in order for a third party to provide services to the party responsible for the file. The special feature of this type of access is that it is not considered a communication or transfer of data, and therefore does not require the consent of the affected parties in order to take place.

However, one essential condition for the service to be provided is that the processing of the data by the third party must be regulated by an agreement including (i) the terms and conditions established for the provision of the service by the party responsible for the file, (ii) the purpose of the processing and (iii) the prohibition of disclosing the data to individuals other than the provider. Moreover, the safety measures which the third parties must implement in the processing system used for providing the service must be stipulated.

As regards management of non-computerized medical records, at present the health care centres are increasingly resorting to a practice which involves subcontracting the processing of medical records through so-called outsourcing agreements. Under these agreements, private companies unrelated to the party responsible for the medical records look after the files. These private companies cannot subcontract the storage of the medical records.

Moreover, and in accordance with the provisions stipulated in Article 9.3 of Act 8/2001 of 13 July on the Protection of Personal Data of the Madrid Regional Government, these service agreements for the processing of personal data must be communicated to the Data Protection Agency of the Madrid Regional Government prior to their execution.

2. Purging

Once a year, and according to the criteria laid down by the Central Commission for Clinical Documentation planned by the Group of Experts in Clinical Information and Documentation or any equivalent body that may be created under the future regional Act, the UNADC or equivalent service shall make a proposal for the purging or destruction of medical records corresponding to concluded episodes which have been in existence for a period greater than that established by the legislation in force as minimum and mandatory for keeping medical records, as well as those data whose preservation is deemed advisable owing to their epidemiological, scientific or educational value.

After examining the proposal made by the centre or institution, should the destruction of the proposed documentation be approved, it shall be carried out with sufficient internal or external means and with the assurance that the confidentiality of the information will be kept and it will be effectively destroyed, under the responsibility of the UNADC or equivalent service.

Should a decision be made to keep certain information owing to its epidemiological, scientific or educational value, the patients' identification information shall be destroyed in all cases, and only the dissociated clinical and health care data shall be kept, so that it is not possible to obtain the identity of the patient through these data.

3. Transfer of non-computerized medical record data

Although regulated in Article 16 of Act 41/2002 as access to medical records, in fact, and from the point of view of data protection when access takes place for judicial, epidemiological, public health, research or educational purposes, this would be a transfer of data, since access is effected by a third party other than the health centre or institution.

The LOPD establishes as a general rule (Article 11.1) that personal data may only be communicated to third parties for purposes directly related to the legitimate functions of the transferor and transferee with prior consent of the interested party.

However, this general rule shall not apply when a law exists which contemplates the possibility of data transfer. Thus, some legal situations are detailed below in which this general rule, as regards health care, would seriously interfere with the principle of consent to the transfer of clinical or administrative data.

Transfer for conducting epidemiological studies

As regards data transfer for conducting epidemiological studies, the LOPD establishes as a condition that such transfer must be effected as laid down by the state or regional health care legislation.

Act 41/2002 of 14 November establishes that access to medical records for epidemiological, public health, research or educational purposes requires that the personal identification data of the patients be kept separately from the clinical data, so that anonymity is ensured, unless the patients themselves have given their consent not to dissociate the data.

In this respect, Act 12/2001 of 21 December on the Regulation of the Health System in the Madrid Autonomous Region lists as one of the functions of the Public Health Authorities the promotion of epidemiological observation of both contagious and non-contagious diseases, and of all determinant factors in the health-disease process related to the interaction between the individual and the environment, and establishes in Article 55.5 that for that purpose, and subject to the provisions of the applicable state and regional regulations on personal data protection, health related data shall be handed over to the Health Administration of the Madrid Regional Government by the parties responsible for the files, whatever their ownership, when they are required for preventing disease or for conducting epidemiological studies.

Transfer to jurisdictional bodies

Specifically, Organic Act 15/1999 of 13 December on the Protection of Personal Data stipulates in Article 11.2.d) that the consent of the affected party shall not be required when the recipients of the communication or transfer of data are judges or courts of justice in the exercise of their functions.

This legal provision is also described in Act 41/2002 of 14 November, where access to medical records for judicial purposes is regulated, and which establishes that in these cases and when the investigation of the judicial authority is considered crucial, the patients' identification data shall be consolidated with the clinical data.

Consequently, in these cases the judicial request should be justified and should specify the documents in the medical record which are required for carrying out the legal proceedings and investigations, and the centre must send a copy of the documents or provide access to such data within the centre itself.

Transfer to the police

This data transfer situation is not provided for specifically in Act 41/2002 of 14 November, although in fact it is quite common.

Generally speaking, the LOPD regulates this situation separately in Article 22.2 and establishes that collection and processing of personal data by the police for law enforcement purposes may be effected without the consent of the affected individuals as long as the intent of such collection and processing is to prevent an actual risk which might endanger public security or to repress criminal offences.

Being health-related data, Article 22 itself, in Section 3, establishes that in these cases data collection and processing must be effected exclusively in those situations where they are absolutely necessary for the purposes of a specific investigation, without prejudice to the control of the legality of the

administrative action or to the obligation of the jurisdictional bodies to give satisfaction to any wish expressed by the affected parties.

This possibility of collection and processing derives from the law enforcement activity recognized to the police in Organic Act 2/1986 on Police Forces (Article 11).

Consequently and given that the LOPD, being a form of access to specially protected health-related data, establishes that law enforcement activities must be subject to legal control, it is understood that in these circumstances the police request must preferably be authorized by the corresponding judicial body and be justified, with an indication of the documents in the medical records which are required for the investigation, and the centre must send a copy of the documents or provide access to such data within the centre itself.

Transfer to medical inspections

This is another situation where the patients' consent would be excluded, as it is expressly provided for by law.

Thus, Act 41/2002 of 14 November stipulates in Article 16.4 that official health personnel exercising inspection, evaluation, authorization and planning functions have access to medical records when carrying out their functions. Consequently, once the request has been justified the centre must provide access to this personnel.

Data transfer to the Auditing Services of the Madrid Regional Government

The parties responsible for the files in the Madrid Autonomous Region have on many occasions asked this Data Protection Agency whether personal data should be handed over to the Auditing Services of the Madrid Regional Government. The interpretation in this case is that, in accordance with the provisions of Article

11.2 of Organic Act 15/1999 of 13 December on the Protection of Personal Data, the basis of the authority of the Auditing Services to request personal data can be found (i) in Article 82 of the Inland Revenue Act 9/1990 of 8 November enacted by the Madrid Regional Government, under which all transactions, documents and records of the Autonomous Region's Administration from which economic rights and obligations derive shall be audited and registered in accordance with the provisions of the aforementioned Act and its complementary provisions, and (ii) in Article 83.3.c) of the aforementioned Inland Revenue Act 9/1990 of 8 November enacted by the Madrid Regional Government, which establishes that one of the intrinsic provinces of the auditing activity is to request, when the nature of the transaction, document or record to be audited so requires, any legal advice and technical reports deemed necessary, as well as any records and documents needed to conduct this activity.

Transfer of dissociated data

Article 3.f) of Organic Act 15/1999 of 13 November on the Protection of Personal Data defines the term "dissociation" as any processing of personal data done in such a way so as to ensure that the information obtained cannot be associated with any identified or identifiable person.

In this regard, point 26 of Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, establishes that the principles of protection must be applied to any information related to an identified or identifiable person; that in order to determine whether a person is identifiable it is necessary to consider the whole of the means which may be reasonably used by the party responsible for the processing or by any other individual to identify such person; and that the principles of protection shall not apply to data made anonymous so that identification of the interested party is no longer possible.

Insofar as the personal data included in non-computerized medical records are communicated in a dissociated manner, so that such information cannot be identified with a specific individual, they cease to be personal data and, therefore, in accordance with the provisions of Article 2.1 of Organic Act

15/1999 of 13 December on the Protection of Personal Data, no longer fall under the scope of this Act, and such information may be provided without infringing the data protection legislation.

Transfer owing to change of physician and/or health care centre

When the patients exercise their right to change or choose a different physician and/or health care centre, according to the terms and conditions established by the competent health services, the new responsible physician, with the patient's express authorization in writing, may, through the UNADC or equivalent service in his/her centre, request from the UNADC or equivalent centre of the centre of origin the complete original of his/her new patient's medical record. This information would be added to the medical record opened at the new centre, which would be legally responsible for its safekeeping and filing from that moment.