Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Legal Aspects of Data Protection in Medical Informatics

Poullet, Yves

Published in:
Data Protection and Confidentiality in Health Informatics : Handling Health Data in Europe in the Future

Publication date:
1991

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

Link to publication

Citation for pulished version (HARVARD):
Poullet, Y 1991, Legal Aspects of Data Protection in Medical Informatics. in *Data Protection and Confidentiality in Health Informatics : Handling Health Data in Europe in the Future.* Studies in Health Technology and Informatics , no. 1, IOS Press, Amsterdam, pp. 138-160.

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

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

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

Download date: 04. May. 2026

Data Protection and Confidentiality in Health Informatics
CEC DG XIII/F AIM (Ed.)
IOS Press, 1991

Legal Aspects of Data Protection in Medical Informatics

Yves POULLET
CRID, Facultés Universitaires Notre-Dame de la Paix, Namur, Belgium

Introduction

The purpose of this study is to present a description of the legal conditions and demands relevant to the use of electronic memory health cards. More precisely our concern is to determine the minimum conditions necessary to ensure the confidentiality of medical information or, in other words, respect for the privacy of patients issued with the card. Personal medical history has traditionally been regarded as pertaining to the most intimate sphere of the individual.

The Medical Data Card (MDC) can be considered as a sort personal medical identity card. It may be described more technically as a plastic card incorporating either a microchip or laser technology capable of recording medical information without record to a network. The principle of the card is as follows : each patient carries his own medical data accessible in all or in certain medical centers. The patient is thereby, and this is the point at which the card is fundamentally innovative, the owner, in a material sense, of medical and administrative data concerning him, even though he may not necessarily know the precise contents.

Other cards may come into existence ; there is talk of a card for medical professionals which will enable the same, under certains preconditions, to have access to the medical content of the MDC. We are analyzing only the patient's card.

The advantages of the patient'MDC are primarily in the area of logic : the rapidity of treatment can be noticeably increased, particularly in cases of urgency. Furthermore, the patients benefits from a greater freedom in the choice of his doctor without the latter, as was formerly the case, having to open a new file. Finally, confidentiality of the data, if well organized, can be better assured, while errors of transcription can be markedly reduced.

The principle difficulties raised by the introduction of such a card can be summarized by the dilemma represented by the necessity of rapid access to medical information and the virtue of respecting the confidential nature of the same.

The difficulties concern essentially the following area :
- the violation of medical secrecy ;
- medical responsibility : reading the card may encourage a doctor to dispense with a conscientious examination of the patient ;
- misguided purpose : the medical information could be put to unethical uses ;
- discriminatory practices : such as a closed network of health care where only those in possession of a card are eligible for treatment ;
- safeguarding the free choice of doctor by the patient ;
- the liberty of the patient to communicate his card of not to different doctors participating in his treatment (guaranteeing his right of self-determination) ;
- the security, reliability and technical limits of the system and consequently the liability of his creators ;

- the risk of destruction of modification of the medical information, whether intended or not.

I THE MEDICAL DATA CARD AND THE QUESTIONS AT STAKE.

The questions at stake of an MDC are twofold : what are the contents? Whose interests are involved? These are the two questions that we propose to study in this first part.

1.1. CONTENTS

1.1.1. The distinction between internal and external contents

A. External contents

By 'external contents' are understood all information contained on the card in a legible fashion without recourse to any technical procedure. This information has the function of identifying the bearer of the card.

Name and first name are not seen as sufficient to guarantee the material identity of the bearer, that is to say, that the person presenting himself as the bearer is in fact the card's rightful owner. The enclosure of a photograph or the requirement to simultaneously present an identity card offer a better guarantee in this respect.

Such information permit in case of loss or theft the retrieval of the person concerned without recourse to technical means, thereby avoiding the reading of the internal contents. But one may ask, to exclude all risk, if it were not preferable to indicate on the card solely the institution responsible for its issue. Thus the card would be protected from prying eyes.

B. Internal contents

By 'internal contents' are understood such data as may only be read by the appropriate technical procedure (reading device) and having the goal of identifying the bearer and furnishing his medical history (infra).

It is at this level that the most acute problem is presented, namely the necessity of finding a balance between a respect of individual liberties ant the requirements of accurate medical data.

1.1.2. Distinction in function of the records contained

The card permits the regrouping in a single source heterogeneous elements which were formally dispersed such as :

- hospital records, or all information pertaining to the specific function of a hospital in provision of health services. This data is under the responsibility of the hospital director ;
- family doctor's records ;
- medical pass book ;
- administrative records.

Note that only the medical pass book is currently accessible to the patient. But it is rare and does not exist in all countries. In Belgium, for example, young children have a vaccination book.

The revolution takes place at the following level : we are moving from the storage of a record localized in one place and held by one person to a mixture of records. The principle innovation of the MDC resides in the assembling of an individual dossier where are to be found all medical and administrative records formerly kept by autonomous instances.

1.1.3. Distinction between administrative and medical contents

One can distinguish between the primary data created by the granting of the card and the subsequent data arising from the use of the card. The first, administrative data, are inscribed on the card at the moment of issue and are hardly or not at all subjects to modification. The second, medical data are inscribed on the card at intervals as treatment progresses.

A-Administrative data

These regroup information relative to identification, social insurance and eventual complementary cover. Thus appears a minimum of information necessary to identification, name and first name of patient, sex and birth date.

A difficulty arises at the mention of the insurance number. Certain national legislations could consider this information as sensitive and as a result forbid its mention because it refers indirectly to the philosophical or political opinions of the bearer[1].

This data are used when admitting a patient to hospital or consultation.

We remark in passing that the possibility is not excluded that administrative data concerning sick insurance, places of hospitalization, former admissions to that service or that hospital,could influence the quality of care provided.

The nature of information collected depends after all on the nature of the user.

B.Medical data

Medical information is recorded on the card as an assistance to treatment.

Its content is by nature very varied. A first attempt at classification establishes the distinction between objective and subjective data. For example, weight, age, sex, height may be considered as objective data. As subjective data may be considered the results of physical examinations, soundings, data generated by machine (electrocardiographic, scanner, x-rays), data from interpreting commentary (radio diagnostic, diagnosis of ECG) and data from hypotheses advanced by one or more doctors using there personal capacity for analysis. Such data may all be considered subjective to the degree that they require an interpretation on the part of the doctor.

The distinction we have just proposed is based on the necessity of dividing the data into two separate lists. It is nonetheless difficult to trace a clear line between these two categories.

A second possible distinction founded equally on notions of objectivity and subjectivity develops the idea in a different manner. It ranges on the side of subjective data all information pertaining to the patient's medical history. This classification is also not totally satisfactory. Information bearing on the history of a patient is of such importance as to be classified as objective.

Let us take as an example data connected to inherited genetic characteristics (see, in this connection, the current situation in Holland) termination of pregnancy (excluded by the CNIL except with written permission of the card bearer), alcoholism, drug addiction, mental illnesses, sero-positivity in AIDS trace tests, etc.

[1]The newly draft bill in Belgium for the protection of privacy in matters of personal data forbids the processing of data of a personal nature relating to opinions pertaining to the choice of such insurance.

We ask ourselves further whether the criterion of free and informed consent suffices to justify the mention of such data on the card.

Whichever one chooses, no distinction will ever be entirely satisfactory inasmuch as some information is more sensitive than others, as is the case, for example, with psychopathic conditions.

This problem well illustrates the difficulty in determining the pertinent criteria for categorizing the information to be recorded on the card.

One last distinction enables us to introduce the second area of risk : the persons involved.

1.1.4. Distinction relative to target groups

Good sense leads one to think that an MDC system will rapidly embrace the entire population. Such a general diffusion will be conducive to increasing the efficiency of the system. Indeed, the smooth functioning of the system depends upon a sufficient number of scanning devices, and only a massive issue of card would be justify a sufficient diffusion of scanners.

However, that may me , limiting the target groups is currently the most practical approach (the aged, pregnant women, diabetics, ...). From this point of view the desired goal is more effective surveillance of a particular risk group.

1.2. THOSE INVOLVED AND THEIR SPECIFIC INTERESTS

Medical data cards are of interest to a certain number of persons. Each has his specific preoccupations, first the users of the service (health care personnel-patients), then the providers of the service and then the people who gravitate around any of these.

1.2.1. Parties to the basic transaction : health care personnel-patients

A-Card users

Variety is without doubt their principle characteristics. One may, however, distinguish between doctors, health professionals who are not doctors, and those whose work revolves around heath professionals.

- The members of the medical body : the doctor directly associated with the treatment or his replacement, general practitioner or specialist, the doctor working in a hospital - more and more frequently part of a team - doctors working at home - individually or in association - medical biologists, insurance company doctors, company doctors, the doctor called upon for legal opinion...

- Health professionals other than doctors, chemists, physiotherapists, dentists,...

- Other personnel in the health care institution : hospital personnel, medical and paramedical personnel, whether in clinical or domestic services, administrative personnel,...

The interests of health care workers are directly connected with the services rendered whether in treatment or emergency. In any event, this adaptation can be more particular, as in the case of a medical biologist for whom the medical data on the card may be of use in determining what sort of analyses it would be appropriate to make.

For health care workers the card raises a double difficulty. Firstly the patient is always in

possession of his entire medical record whereas the former system permitted doctors to limit the information longer in a position to know exactly to whom he is divulging the information he records on the card. Thus the doctor loses a part of his control over the information.

B. Beneficiaries
By beneficiaries are here meant carrying the card, whether they represent the entire population or only a particular sub-group of the same.

Their principle interest is the quality and rapidity of the medical care they receive.

In this respect the data card avoids both the necessity of opening a new medical file and the transfer of the same by each consultation with another doctor, which facilitates the continuity of treatment and permits a patient to change doctors without difficulty.

However, the use of the card is no neutral matter for the patient and poses certain difficulties.

First and foremost, the patient may not necessarily wish the doctor he consults to be aware of his whole medical history.

In reply to this preoccupation : the patient chooses to give or not to give his card and thus decides to a certain degree who may receive information concerning him. In this way the patient would seem to have to a certain degree to be assured of his right of self-determination (infra).

Nonetheless, this assumption is relative when one places the relation-ship doctor-patient in its context. Such a relationship is of the type 'specialist-uninitiated' and may as a consequence demonstrate a certain lack of equality? In practiced it would appear rather difficult for a patient to refuse his card to the doctor who asks for it, inasmuch as such a demand serves a medical purpose and not malicious curiosity.

1.2.2. Those who issue the card

The host could be an industrial supplier, an administrative office, doctors, or a research center. It could even be a combination of any or all of these. The actual makers of the card occupy a privileged position both as material suppliers and as those responsible for the system's logic base.

It would seem essential, whatever the composition of the host, that the latter contracts, within the framework of its functions, to guarantee respect for the principles of medical ethics and to ensure the global security of the system.

Indeed, the principle functions of such hosts, consist, on the one hand, in the allocation of the cards and the means of access both in reading and recording, and on the other hand, in the development of an system enabling those authorized to connect with one another by means of a telecommunications network.

Those issuing the card must, within the framework of these functions, be held responsible for the performance of the system, its eventual malfunction, the unethical uses to which it could be put, and , in a more general manner, for its security and reliability. Furthermore, it is indispensable that a certain normalization of hardware and software be achieved, if notably to free both doctors and patients from being bound for better or worse to one particular service center.

1.2.3. Persons peripherv to this relationship

A.Government authorities

The preoccupation of government authorities is with the politics of public health and the reduction of health costs. Do these preoccupations justify even the most limited access to the MDC
and the keeping of a summary file of card holders ?

B.Health insurance institutions

More precisely, the sick insurance department of the Social Security, the Mutual Insurance Funds, and the private insurance companies.

The goal sought by these organizations is principally the reduction of costs. The data card could be notably useful as a basis for the reimbursement of health care charges.

Does this goal justify the fusion of the current social security card with the MDC ? Wouldn't a reference to the paying institution sometimes present a danger with regard to the law for the protection of personal data ?

C.Ethical institutions and/or medical unions

These are concerned for the respect of professional ethics and more particularly in protecting the interests of health care professionals.

They may be enabled to play an important function in this regard in the matter of controlling the smooth functioning of the system and in that which pertains to the distribution of cards controlling access entitlement and authorization for health care professionals.

D. Employers [1]

Employers are interested in the contents of a medical dossier for two reasons. Firstly when selecting a candidate for a job in order to know the state of health of the candidate employment and secondly to arrange the conditions of work with regard or in response to the health of the employee.

E. Judicial authorities [2]

The data card can serve as evidence in private litigation of criminal prosecution. One can also imagine that some would wish to use it in establishing questions of paternity. One may envisage, insofar as the card contains entries that are signed and dated, that it would serve to determine the physical presence of a doctor at a certain time and place. And finally it would seem likely to us that certain people would use it to determine the responsibility of a doctor, be it in relation to professional misconduct or to prove negligence or fault connected to the use of the MDC system itself.

F. Institutions for medical research

Although not participating directly in treatment, research institutions play a key function in improving the quality of health care.

[1] current or future
[2] civil and penal suits

The information contained on the card may serve on the one side for the purpose of medical research and on the other for the control of populations considered at risk or for disease prevention. The MDC system offers in that respect a double advantage. Firstly it permits, inasmuch as the totality of medical data is conserved on the card, to retrace the patient's complete medical history or at least its salient points, enabling the evolution of the patient's health to be suveyed. Secondly, it represents treatment data already processed and partially centralized by the service center pertaining to an entire population or a large sample of the same. The partial centralization realized by each service center must remain partial to avoid a too great centralization in the research laboratory.

II Existing regulations applicable to Medical Data Cards

The first part of our study attempted to define the principle areas of risk connected with the introduction of an MDC system. In this second part we are concerned to pinpoint the applicable regulation, taking into account the general principles of the privacy laws and the ethic of professional secrecy, while delineating specific regulations and principles already elaborated
in France in this connection.

2.1. GENERAL PRINCIPLES

2.1.1. General principles derived from the laws of privacy

The Convention of the Council of Europe of 28 January 1989 relative to the protection of individuals in the cas of electronically treated personal data furnishes some general principles, accepted by the majority of states in the Community, which assure the protection of confidential data and thereby respect of privacy. We propose to analyze the different principles of the convention with regard to MDCs.

The collection of data by fair and legal means is covered by article 5a. This latter is based on the idea that the patient must be fully cognizant of the individual information gathered concerning him, and secondly of the purpose it is intended to serve. It cannot, therefor, be permissible that a card contains information of a secret or coded nature without the bearer's knowledge.

This is a matter of informing the bearer of all those who have access to his card whether reading or recording.

A. Articles 5b et c prescribe respect for the principle of finality in the gathering and employment of data.

On the one hand, data should only be gathered in proportion to the needs it serves. The only purposes permitted to justify the registration of data are relative to the admission or treatment of the patient. The gathering of socio-economic data (salary, profession,...) is, to the degree that it does not fulfil these requirements, proscribed.

Furthermore, as the data may not be used to serve a purpose other than the one for which they were gathered, it is necessary to clearly delineate the finalities.

The data is stocked and transmitted with a view to assuring effective health care. More precisely, the data must facilitate the treatment of the patient -also by case of emergency-

and the continuity of the same, while the administrative data must serve for the admission of the patient to a hospital or consultation.

The question of whether the informed consent of the patient should be regarded as sufficient to permit the data to be used for some purpose other than these just mentioned will be examined later.

Finally one must observe, that the data should be structured in such a way a to serve these different purposes (administration, emergency and treatment.

B. Article 5d is concerned with the quality of data. These must be exact and kept up to date. This relies on the responsibility of the doctor in that which concerns data storage, the responsibility of the patient who by choosing not to present his card must thereby accept that it cannot be entirely up to date and the responsibility of the programmer in that which concerns the conception and functioning of programmes.

C . In conformity with Article 5e data may not be kept beyond the period necessary to serve the legitimate goals of treatment. The question raises itself as the whether it is not necessary to conserve medical data for a sufficiently long period.

D. Article 6 forbids the processing of various 'sensitive' data unless the national laws furnish the appropriate guarantees. Medical data fall into this category.

Their collection and procession must be made in accordance with the principle of pertinence developed above in point A.

E. The principle of data security enunciated in Article 7 is intended to protect data from accidental or unauthorized destruction or loss, unauthorized access, alteration or dissemination.(to the card or by intermediate of the host)

F. Article 8 grants every individual[1] the right of access to and correction of all recorded data that concerns him. Taken from there, this right is applicable to medical information. Certain limits[2] however may restrain the exercise of that right.

Firstly, it is not always desirable that the patient has direct access to the medical dossier on his MDC. However, if the right of the patient is limited he still retains the right to receive an intelligible summary of the same from his doctor. This mediation offers a triple advantage :

- the accessing of data takes place within the framework of a confidential relationship between doctor and patient ;
- the communication of data is to a certain degree adapted to the patient inasmuch as diagnoses of a grave or fatal[3] nature are only communicated with reference to the mental state of the patient;
- medical secrecy is safeguarded inasmuch as access, even indirect, by unauthorized persons cannot occur.

Finally, such limitations may bear upon the patient's right or rectification. Such is notably the case if the rectification demanded is contrary to the observed medical situation.

---

[1] Debate in France at the CNIL : has not the patient, as material owner of the card, the right to know the contents of his dossier ?

[2] Problem : Article 42 of the French code of medical ethics authorizes a doctor, as a matter of medical prudence, to conceal from his patient information relative to diagnoses of a grave of fatal nature. In Belgium Article 33 requires him to reveal his prognosis to the patient. A grave prognosis may however be legitimately concealed from the patient, and a fatal one may only be revealed to him under exceptional circumstances.
In the same manner it is sufficient that the card be incomplete. The doctor simply does not record on the card those pathologies that he does not wish the patient to know.

[3] reference in French law

2.1.2. Professional secrecy

A. Principle

Data covered by professional secrecy must remain confidential if recorded by persons bound by cath and in conditions in which the latter is applied. The fact that the patient is the bearer of this data need make no difference to the application of this principle.

The obligation of secrecy reposes upon the privileged relationship established between doctor and patient. It extends over all that the patient reveals within the framework of the relationship and, more widely, over everything observed or confirmed by the practitioner.

Such an obligation of secrecy[4] is founded both on the interests of the patient, and on the collective interests of general health relative to good medical practise. Basically, the patient must be able to confide unreservedly in those who care for him, speak freely of his history and of the symptoms he has felt.

This rule of secrecy is to be found in all the European legislations. By way of example we shall present in some detail the regulations current in Belgium and France.

In Belgium, Article 458 of the penal code requires that a doctor or any person holding secrets of state or profession that have been confided to him is liable to penal sanction in the event of his revealing the above, except when called upon to testify in court or when the law otherwise obliges him to reveal the same.

Article 55 of the code of medical ethics obliges a doctor to observe professional secrecy in all circumstances. The legal exceptions are delineated by the same code under article 58.

In France, professional secrecy is imposed on all doctors in the interest of the patient within the conditions established by law. Article 378 of the penal code prescribes penal sanctions against doctors or other health care professionals who have revealed secrets confided to them in their professional capacity. Article 89 of the code of medical ethics is similarly phrased.

B. Trustees of the secret

The reading of medical information, to be in conformity with this principle, must be confined solely to persons bound to silence.

The latter are generally doctors and those involved directly with treatment. In that which concerns the second category a certain gradation of obligation to secrecy can be observed in the various national legislations.

For certain professions such a psychologists or social workers, professions engaged more indirectly with treatment, a certain ambiguity persists.

Those not normally engaged in treatment (ancillary and administrative staff, insurance personnel) are not normally bound by the obligation of secrecy.

C. Persons with regard to whom there exists an obligation of secrecy

1. With regard to the patient

It is generally admitted that there exists no obligation of professional secrecy toward the patient, on the contrary, the latter has a recognized right, to information although this right may be limited in certain cases[1], notably where knowledge of the diagnosis could have a detrimental effect on the physical or mental health of the patient.

[4] F.WARRANT, 'Confidentialité du dossier médical informatisé', 27 mai 1989

2. With regard to the third parties

a) In general

It is clear and evident that there exists an obligation of secrecy toward third parties. Nevertheless, the revealing of secrets may be condoned in certain cases if it is made in the best interest of the patient or if exists a legal obligation. But this divulgence even in the interest of the patient or if prescribed by the law must limit itself to that which it is indispensable to reveal .

The tacit authorization of the patient does not remove the obligation to secrecy.

According to certain sources , even an explicit authorization does not suffice to allow the revealing of medical information.

Note that the obligation of secrecy persists even after the patients decease.

b) Particular cases

- toward administrations. The law enumerates and limits the cases where a secret can be divulged ;

- toward tribunals.
Professional secrecy is not at the disposition of the patient. The fact that the patient may have delivered his doctor of the burden of secrecy does not oblige the latter to divulge, even in court, facts covered by medical secrecy .

- toward medical research institutes.
Medical secrecy is not violated if the patient is not identified, the principle of secrecy does not apply to the illness per se but rather to its relation with a distinct individual.

C. Sharing the secret

The secret may be shared in the interests of the patient when ensuring the continuity of the treatment.

Sharing is generally admitted between the hospital doctor and the family doctor. On the other hand, such sharing is for example accepted with regard to doctors employed by insurance institutions.

Beyond this, the sharing of data often is a simple matter of fact resulting from teamwork situations common in clinics and large practices.

2.2. PRINCIPLES APPLICABLE TO MEDICAL DATA CARDS

Before responding to the challenges posed by the card, we propose to revue the norms specifically applicable in this domain. We shall open with the Recommendation n° R (81)

[1] In France according to article 6 of the law of January, 6, 1978, a doctor may choose that which he reveals to his patient, nd according to article 42 of the code of ethics he is authorized to not say everything.

of 23rd January 1981 elaborated by the Council of Ministers of the European Council relative to the regulation applicable to automated medical data banks. Afterwards we shall look at the essential principles delineated by the CNIL (Commission Nationale Informatique et Libertés) resulting from the experience gathered in France since the introduction of MDCs.

2.2.1. Recommendation of the committee of ministers of the European Council, 23 January 1981, relating to the regulation applicable to automated data banks

These regulations, although not constituting a normative statute in law enunciates the important principles that the member states must needs respect when framing their national legislation.

The applicability of this convention rests on two points :

1. the card represents a miniature data bank and
2. its finality is clearly that of medical treatment.

We shall only deal here with the principles relating to the intrusion of MDCs.

The Recommendation delineates above all (point a) the necessity of subjecting any medical data bank to its own specific regulations, whose parameters are defined elsewhere. It also treats of the principles relative to both registration of and access to data. Finally, the explanatory report mentions the necessity of a major campaign of public information which would seem particularly desirable before introducing a system of Medical Data Card.

A. The regulation of data banks

Regulations, established in conformity with the laws of the State concerned (article 1.4 and 1.5 of the Recommendation) must comprise among other things, precise provisions as regards the following :

- distinct rules adapted to cases where the data bank contains several series of medical files or sub-systems of medical data;

- (article 3 of the annex) the specific purpose of the data bank, categories of information recorded, the physical person or institution on whose account the data bank is kept;

- categories of people authorized to record, modify or erase data; the parameters of access to the data bank and of the communication of information to third parties or persons concerned and also the procedure relative to demands for the use of data for purposes other than those for which it was collected;

- the conditions under which, should the need arise, the data bank may be permitted to connect with another data bank.

B. The recording of data

The text takes up in detail (article 4.1) the principles of the European Council such as :

- collection by fair and legal means;
- the collection only of data adequate and appropriate to the stated aims;
- the exactitude (verification within the limits of the possible) of the data and its actuality as regards the needs it should fulfil.

The inexactitude of data can indeed cause considerable damage. But, on the one side, the technique of cross-checking may be used in order to minimize the risk of error, and on the other, the data recorded on the card is always subject to review by a doctor. Keeping a medical record up to date is justified in the light of the necessity of continuity of treatment.

The text adds (article 4.2) a principle specific to medical records, which is the necessity of structuring the files in such a way as to guarantee the possibility of selective access and the security of information. This obligation must be imposed on the designers and producers of cards.

The files must also as a general rule be subject to separate classification of identification data, administrative data, social and medical data. A distinction between subjective and objective data should also be affected in the last two categories.

We must recall at this point the difficulty of determining what is subjective and what is objective in the classification of medical data.

C. Access to data

Primarily, access should be reserved, as a general rule, to doctors (article 5). However, in conformity with national legislation, this access could be extended to include paramedical personnel. In any case, no one should have access except to that information pertinent to the exercising of his specific task (article 5.3), neither may he make use of that access for a purpose other than that for which he is authorized .
Exceptions are made to this principle inasmuch as the information is rendered in a form which makes the person concerned unidentifiable or when the different usage results from a legal obligation (contagious diseases ...)...

Finally (article 5.4.) , neither the existence nor the contents of a medical dossier may be communicated to third parties other than persons or institutions occupied in the fields of medical care, health or medical research except in cases where the laws of professional secrecy permit.

D. Public information campaign

The expose of motives adds to this recommendation the necessity of a campaign to inform the public of the existence or development of a medical data bank. This knowledge should make it possible for those whose interests are affected to make their point of view known and, particularly in the case of a data bank in the process of development, to do so before the sums invested have become too important.

2.2.2. General principles of the CNIL

At the time when opinions were given concerning experiments with cards, the CNIL placed the accent more particularly on the following recommendations resulting from the lack of transparency of electronic memory cards.

A) Respect necessity for the rights of the persons involved in the experiment;

B) Security devices to guarantee, in full confidentiality, access to the data only by medical personnel specifically authorized to that effect;

C) Study the effect of the use of MDCs on the practice of medicine, on the relationship doctor/patient, on the application of medical secrecy and ethics.

Taking into account the necessary respect delineated above).

1. Voluntary nature : the users -professionals and patients- must be allowed the freedom to participate or not in the seting up and functioning of the system. No penalization may

be consequent upon a refusal to participate.

2. Free and informed consent to the use of the card. Patients and doctors must be clearly informed of the purposes and parameters of the system, the method for inscription and erasure of data, the persons authorized to read the information and the rights and means at their disposal. The initial consent of both parties la reinforced by the restatement of that consent at each application of the DC system; the patient disposes of the freedom to refuse to present his card or to refuse access to certain types of date (confidential codes for particular kinds of data ...).

3. Exclusion of all discrimination between bearers and non-bearers of the card,, whether doctor or patient.

Above all the introduction of a MDC system may not limit or restrain the patient in his choice of a doctor .

Finally, a doctor who participates in the MDC system may not refuse to treat a patient who either does not participate in the same or who refuses to produce his card.

4. Necessity of good information in communication between doctor and doctor or doctor and patient.

III. TOWARD A NEW NORMATIVE FRAMEWORK

Preliminary reflections

The electronic data card has sometimes been considered as the solution to the dangers posed to our liberty by the computerization of our society. It represents, at least in appearance, a reappropriation by the individual of information concerning his own person : the individual would retrieve control of whether to communicate or not the image of himself given by the date on the card to others. Some go so far as to say that through the electornic card a person once more becomes again the owner of his own data.

This "control" risks being illusory and the "ownership" a mere appearance in the measure :

a) that the written data is reproduced somewhere else :

b) that the individual does not control the content of the dossier he himself carries;

c) that, to take up the comparison with data banks constituted outside the control of the individual, access to which, frequently compartmental, is rigidly controlled by the director of files, the electronic data card risks creating a right of access to the complete dossier, to readers of whom some could put pressure on the bearer;

d) that not only would newly inscribed data be subject to less control than that envisaged in the case of a conventional data bank, but furthermore, inasmuch as the content of the card would seem to present an objective and reliable appearance, the card would risk becoming the basis for a chain of errors potentially damaging to the bearer.

One can easily conceive that the introduction of electronic data cards in the domain of health care could amplify the range of this criticism.

However, it may seem from these preliminary conjectures, it is not our intention to condemn the use of the MDC, but rather to underline the importance of a regulatory

framework capable of reducing the risks created by this new technology and of reinforcing interest is this alternative to centralized data banks.

The presentation of our recommendations relative tothis framework follow a crhonological plan :

a) the setting up of a system to process MDCs;
b) the issuing of the cards;
c) the contents of the cards;
d) reading the card;
e) writing the card;
f) the renewal, destruction, or withdrawal of the cards.

3.1. SETTING UP OF A SYSTEM TO PROCESS MDCS

The choice of a system supposes as previously resolved a number of technical questions of which the importance is considerable since they condition the safeguardind of the confidentiality of the data involved. Without being exhaustive, let us indicate the following :

- the type of MDC : according to the technology chosen, the capacityu of the cards may differ appreciably. The distinction of separate zones of acess would or would not be possible and the method for verification of data recorded and of persons authorized either to read or to record new data would vary;

- the terminals and software : depending on the price, the standards, and notably the compatibility, the possibility for doctors to equip themselves to be able to read any kind of card would be more or less large. The choice of standards already internationally established would permit a larger utilisation of the MDC;

- the normalization of data featured on the card -more an administrative than a technical question- the normalization of particulars if such exist and are widely accepted will further enlarge the circle of those capable of understanding the contents of the card;

- the security measures necessary to protect the confidentiality of data;

- the system of communication between different (?) and the processing centre must be foreseen in such a way as to ensure that in case of loss or deterioration rendering the card unreadable, a regeneration of the card would be possible even at a distance according to appropriate procedure.

The system of processing would have the following essentially administrative functions :

- the issuing of the cards (direct delivery or through the medical system) and of secret numbers to enable the card bearer to author-ize the doctor of his choice to read the card;

- the authorization (delivery of access systems) and the process of verification of persons authorized to have access to the card contents;

- the process of renewal of the MDC at the expiry of a fixed period or unpon loss of the card;

- the eventual rendering anonymous, within the framwork of its being used for research purposes by the processing authority or by third parties, of all current or successive data on the card.

Some recommendations seem to us to be appropriate to the introduction of a system for processing MDCs. Certain of them are directly taken from the Recommendations of the

European Council, 23rd January 1981, relating to medical data banks (see above, n. 2.2.1.)

Recommendation 1 : Principle of regulation of each processing system

Each processing system will establish its code of regulations, specifying the different technical and administrative characteristics of its system (concerning these characteristics see above list), the security measures taken to asure the confidentiality of the card, and finally, the processing measures necessary to assure respect for medical ethics (e. g. within the processing centre, access to medical data would be reserved solely to doctors bound to professional secrecy).

Recommendation 2 : Principle of dual control of regulations

Each system will submit its regulatory code, firstly to the authorities responsible for the monitoring of ethical principles and secondly to those authorities responsible in questions of data protection. This double control should take place not only at the system's inception but throughout its period of service and particularly in event of modification.

Recommendation 3 : Principle of the publicity prior to the existence and development of MDC processing systems

Parallel to the recommendation already made by the Council of Europe with regard to data banks, the necessity was added of previously informing the public of the principle characteristics of the system in process of development (objectives, extent, type of data to be handled, type of patients targeted, etc.). This infomation would permit those in interested quarters to make their point of view known before significant levels of investment had been reached (see above, n.2.2.1.).

Recommendation 4 : Principle of the structuring of the card

The necessity of structuring the card in different zones of access, in order to assure selective and/or limited degrees of access, must be affirmed (cfr. parallel to the principle applying to data banks, see above, n.2.2.1.). There must at least be a separation between identification data, administrative data and among the medical data, a section for emergency data.

3.2. DELIVERY OF THE CARD TO THE PATIENT

There seem to be two quections which must be posed.

Firstly, should delivery to the patient be effected directly by the processing organization or through the intermediary of a doctor who would alone know the precise carrier of the card, the processing centre only knowing the identification number?

Without wishing to quench the idea of delivery by the processing organization, we would like to draw attention to the fact that this solution places in the care of the processing body some important responsabilities of security and confidentiality.

Secondly, the delivery of the carddemands significant precautions in order to respect the principle of voluntary affiliation and free and informed consent enunciated by the CNIL.

The respect of these principles justifies the following recommendations:

Recommendation 5 : Necessity of informing the patient thoroughly prior to issuing the MDC

The information of the patient is conceived with regard to the purpose, nature and modus operandum of the system, the contents of the car (nature of data stored), the individuals

authorized to read or record data , the procedure tofollow in event of loss either of the card or of one's personal code number (Personal Indentify Number), the means of access to the card's content (see section below) and the right to refuse access to data on the card.

This act of thoroughly informing the holder should be the duty of the person assigned to deliver the card.

Recommendation 6 : Necessity of free consent to the issuing of the card

This recommmendation seems to us to have dual significance: the first bears on the fact that the delivery of the card may not either directly or indirectly, be in any way construed as a condition of access to medical services; the second makes clear that a document explaining the essential information delineated above in recommendation number 5 should be submitted in duplicate to the patient for signature, one copy to be retained by him.

3.3. THE CONTENT OF THE MDC

The introduction distinguished, in the case of the card, between different categories of data in accordance with certain distinct and complementary criteria.

The first criterion distinguished between the data actually visible on the card and that requiring an access code. Evidently, the external content of the card must be kept to a minimum. We recall that even simple identification data may, as in the case of affiliation to a particular health institution, be regarded as protectable. Furthermore, there is always the fear that, in the case of loss or theft of the card, a person, icluding someone close, might identify the vearetr and endeavour to read the contents. Recommendation 7 may be therefore framed as follows :

Recommendation 7 : Guarding the anonymity of the MDC exterior content

It would be preferable that the exterior of the card carry no nominative information. A simple reference number and the address of the issuing institution, to enable the card to be easily returned, would suffice.

The second criterion concernd the type of files kept by the card. Recommendation 4 proposed already the structuring of the card. Beyond that, should one limit the number or type of dossiers heis ? Without going into questions of memory capacity, a priori, one must recognize that every type of medical file, inasmuch as it merits being dept up to date, should be present on the card. This excludes such dossiers for which a follow-up is unnecessary, for example : a voluntary interruption of pregnancyà of a surgical nature, having no further historu).

In this respect, it is relevant that the patient should know the types of file likely to be kept on the card and be able to freely oppose thge inclusion of this or that dossier, except in the cases of data valid in emergency treatment. Indeed, the failure to record emergency data, such as an allergy to a particular drug, or epileptic tendencies, could result in an incorrect diagnosis on the part of a doctor inclined to rely on the information givent by the MDC.It is therefore important that emergency information be accurate, up to date and, as far as possible complete. The legitimate refusal on the part of the petientto have certain emergency indications recorded on the card, for example drug dependence or AIDS, must result in the Withdrawal of the card.

Recommendation 8 : Principle of transparency of the contents

The patient must be able to know the type of files held on the card. He may oppose the inclusion of data, under reservation of that described by recommendation 9

Recommendation 9 Definition of emergency data and regulations pertaining thereto

Under "emergency data" are to be understood all kinds of information whose ignorance on the part of the doctor could have a gravely prejudicial effect on the health of the patient.

Emergency data must be separately accessible. They must be accurate, up to to date and complete as possible.

The patient may not oppose the inclusion of emergency data excpt insofar as he refuses the MDC itself.

Finally, the notion of administrative data accessible to ancillary staff must ve clarified. If one gives the MDC a finality purely connectec to the continuity of treatment , the inclusion among administrative data of, for example, refular stys at a known psychiatric hospital could be dangerous. If the administrative data appears in a zone accessible to a larger public than health care personnel, its content must be limited to the minimum data necessary to assist the administrative process, without reference to such former history.

3.4. READING THE CARD

Under this rubric, different questions emerge :

- Who is authorized to read the card ?
- Is this authorization total or partial ?
- Haw does this reading function ?
- Has the patient the right to know the card's contents ?

3.4.1. Authorization of health care professionals

The first recommendations are general. Regardless of which health care professional is authorized, it seems important to us that the issuing of an personal identify number for reading or inscribing should follow strict regulations, the object of the following recommendations :

Recommendation 10 : The principle of liberty

This principle echoes recommendation 6. No health care professional may be forced either directly or indirectly to participate in the introduction and use of a MDC system. No discrimination whatsoever may result from a refusal of the same.

Recommendation 11 : The existence of a specific engagement to respect the rights of the bearer

Authorization must be conditioned upon the signature of the health care professional appended to a promise to respect the legal and ethical rules pertaining to the rights of the bearer.

Recommendation 12 : The monitoring of authorization by the ethical institutions of the profession

It would seem necessary to dissociate the functions of responsibility for the system and of authorization cards. This latter function should be under the control of the ethical institutions of the profession which, should the case arise, would be able to withdraw that authorization and charge the issuing authority to put into action such measure ax would assure the efficacy of such a sanction.

Further reflections about the persons to be authorized and the extension of that authorization

A first reflection bears on the possibility of authorizing health care professionals other

than doctors. Although it seems evident that an authorization of access to identification data and the inscription of details concerning administrative data, such as hospital registration, report of a domestic visit prescribed by the doctor, etc, would appear acceptable, the issue of access to medical data, even emergency data, is debatable. The principle at issue is that, even in the case of central data banks, access for paramedical personnel is always through the intermediary of a doctor who specifies the data to be communicated to the paramedic thus authorized.

Except in the case of it being feasible to create separate zones of access on the card for distinct paramedical professionals, for example : a midwife might have access to certain obstetric data necessary to the smooth functioning of her work, it would appear to us that, in default of specific security measures, paramedical personnels should not have access to the contents of the MDC.

Within the medical profession itself one may question the right to access of certain doctors. Access to data banks is justified in the light of the continuity of medical treatment. Recourse to this finality would seem to deny the right of access to doctors designated as a legal experts by courts of law or other jurisdictions, as well as those employed by insurance institutions or as consultants to employers. For such persons, access to information would have to be through the intermediary , and according to the classic procedures with respect to applicable regulations and ethical principles, of the doctor entrust by the bearer with access.

It would seem to us indeed, that the requirement to present the MDC within the framework of a private litigation or criminal prosecution, for example : to demonstrate mental deficiency in a spouse, adds up to a use of the card outside its prescribed finality, which is that of assuring, in a more safe and effective manner, the continuity of health care.

Recalling ghis finality would seem on the other hand to justify reading access to all medical personnel directly involved in treatment whether or not they are in training.

Recommendation 13 : The refusal of reading access to persons other than medical

Regulations must be arrived at and security measures taken to insure that the access to read medical data on the MDC be strictly limited to medical personnel. Limited exceptions may only justifiably exist inasmuch as they are necessary to and restricted by the finality of health care continuity.

Recommendation 14 : Refusal of the use of the card for purposes other tan the sated finality of continuity of health care

The doctor, with or without the complicity of the patient, may not read the contents of the card in order to :
- inform a current or potential employer upon the patient's health ;
- make an expertise for private litigation or criminal prosecution ;
- ...

3.4.2. The actual reading access

The problem of reading access is a dual one :

- one one hand, it is access to the contents ;	a) the determination of procedures to permit a doctor to have
- on the other hand, it is him.	b) the right of the patient to have access to data concerning

a) The first point requires the following recommendation with regard to the patient :

Recommendation 15 : Principle of reading access authorized by the patient

Apart from emergency data, the medical contents of the card may not be accessed except following a positive act of the patient, such as the punching in of a personal indentify number (in the case of minors this is the function of parents).

With regard to both patient and doctor, we may not that each is responsible for the security of his personal identify number, which he may not communicate to a third party, and which must be subject to technical blockage in the event of repeated incorrect attempts.

With regard to the doctor, in that which concerns his right to copy data from MDCs, it is by no means evident that this right is automatic, but must be subject to the authorization of the patient. In any case, copying is only justifiable inasmuch as it is necessary to treatment.

The right of access to the contents of the card could be coupled-technology permitting-with the right of access by telecommunication to centralized data banks where more complete data on the patient might be stored. Such a linkage is dangerous. It permits the instantaneous reconstituting of a complete medical picture of the individual. It is vital that such a link-up possibility be known to the patient from the start, and that this question be made the object of a particular examination by the commissions responsible for data protection.

b) The second point involves the patient's right of access to his own data.

The conditions of precedent relative to medical secrecy with regard to the patient lead us to make the following recommendation.

Recommendation 16 : Right of the patient to read his own file

If an institution (e. g. a hospital or practicer) has a reading device for MDCs it has to enable the patient, whose card it alters or intends to alter, to read the card. The patient should have the right to have the contents of the information interpreted by a doctor of the institution. The institution should have the right to limit the information to a summary by the doctor. It should restrict itself to a summary if it is to be feared that the patient would suffer unreasonable damage, e. g. to his health, by reading the data card (which might say that he had cancer).

Recall that in our opinion, the patient, having been acquainted with the nature of the data on his card, may, if he chooses, demand the erasure of certain items (other than emergency data). It seems to us that the affirmation of this right of the patient would facilitate the social acceptance of the card.

Recommendation 17 : Right of the patient to call for the erasure of data

The patient should have the right to demand the erasure of parts of the information on the data card from every institution that has made medical entries on it.

The practicer will determine if the erasure of the information is detrimental to future medical treatment.

3.5. Entering information on the card

Input to the card is an essential question. On the one hand, the precision and completeness of the information entered determines the quality of care which may be given to the patient. On the other hand, the apparent objectivity of data on the card and the simple fact of their presence there increase the responsibility of anyone entering data.

Certain recommendations seem to us to impose themselves :

Recommendation 18 : Possibility for any doctor with access to be able to enter data on the card

Certainly, it would be useful if every doctor possessing a terminal ;could introduce new data, whether directly through his terminal, or indirectly by informing the doctor who delivered the card of the need to introduce new data.

Recommendation 19 : Right to correct, complete or bring the card up-to-date

A patient's doctor, should his medical examination suggest to him that certain data is incomplete, incorrect, or not up-to-date, shall reserve the right, after having checked his own findings, of correcting, completing or bringing the patient's card up-to-date.

In the case of uncertainty of the exactitude of the data recorded, he can enter an indication of doubt.

Recommendation 20 : Obligation to "sign" any new access on the card

To all data on the card must be appended the "signature" of the person responsible for the entry.

It is clear that this recommendation would have an important impact on the medical sector since it would more easily permit the identification of the person responsible for an item on the card whose content has subsequently proved damaging to the patient. Recommendation 21 attenuates this as follows :

Recommendation 21 : Principle of insufficiency of information on the card

The fact alone that an item of false, incomplete or obsolete data appears on a card may not exonerate a doctor, who has placed reliance on that information, from his responsibility. His is the duty, within reasonable limits, to make the necessary investigation to ascertain the accuracy of data on the card. In particular he should take care that emergency data are up-to-date.

3.6. Renewal, withdrawal or destruction of cards

3.6.1. Renewal of cards

At regular intervals, or when data to be modified cannot be changed by normal means of access, or of course when the card's capacity is full, the patient may, if he chooses, renew his card. A first question concerns the introduction of the renewal procedure.

Recommendation 22 : Introduction of renewal procedure

The process of renewal of the card should be introduced by the patient's general practitioner, in principle the doctor who issued the card. Should however this be undertaken by the host, precautions to guarantee the protection of data from persons not bound bu the medical secrecy must be taken.

Note that the same rule should apply where data must regenerated as the result of accidental effacement or the impossibility of continued reading access.

The process of renewing the card raises the question of which data entered on the old card should be transferred to the new and beyond that of which data from the old card should be conserved at the host.

To the fist question it is easy to reply that it is yp to the doctor who is renewing the card to decide which data from the old card are still necessary to assure the continuity of treatment.

The solution to the second question is less obvious. It necessitates an elucidation of the systematic functions of the host. Is it conceived as a center of data storage regularly kept up-to-date (q at least at each new entry on the card) and permitting at each access the retracing of a complete medical history of the patient at least for a period equivalent to the time the cards have ben in service ? Would such a storage be justified by the requirements of continuity of care ? In principle, no because such data necessary to the continuity of treatment would be transferred to the renewed card, but it is possible that because of insufficient capacity of the card or for other reasons, such os in the case of illnesses where it is necessary to conserve derailed data about the evolution of the patient over a long period, such a storage could be legitimate.

The conservation of data for the process of scientific research was discussed in our treatise on the areas of risk arising from MDCs. The host may conserve data within the framework of medical research or transfer them to a research center.

The legitimacy of data conservation for such an end is not debatable, but does exceed the original finality of the card of improving quality and continuity of care. Therefore the following recommendation should be made :

Recommendation 23 : Conservation of data

If the host intends conserving data beyond the limit necessary for the continuity of treatment, if must supply a motive for that conservation, assure the anonymity of data thus conserved, and inform the patient thereof;

The latter must be able to oppose this alteration of the finality of the data thus processed.

If a transmission of data is made to a host, the same rules apply. The relationship between the host and the doctor with access to the card may be envisaged in two ways. A first hypothesis is that the doctor sends whenever he chooses copies to the service center and has access whenever he chooses to data on his patient that is stocked at the center. The access could be made directly or through a network.

If such is the case, the following recommendations are useful :

Recommendation 24 : Relationship between doctor and service center at the time of issuing the card

The patient must be informed of all possibility of communication between doctor and service center.

The service center has the duty to guarantee the confidentiality of such transmissions in accordance with the technological state-of-the-art.

In the case where access to service center is possible, clear measures must be taken to determine if the transmission should be restricted to certain types of data in storage or not.

The host has to verify by the appropriate programme, that the data is being transmitted by authorized persons and is not in contradiction with data already in stock. In the event of

new data seeming contradictory, the center must immediately inform the doctor who entered the data and the patient's practitioner.

In the case of confirmation by either of the latter, the new information must be indexed with a margin of doubt. The modified data will be erased after this confirmation.

In cases where transmissions are planned between hosts a reglementation will specify :

- the nature of information likely to be conserved by each host, taking into account that medical data can only be stored at the center to which the patient is affiliated;

- the security measures to be taken to guarantee the confidentiality of the data concerned with regard to the staff of the service centers.

3.6.2. The problem of destruction of the card.

The destruction of the card or of all possible access to the card would be in consequence of :
- the wish of the patient;
- the loss of theft of the card ;
- the death of the patient.

Each of these cases may be to the object of a Recommendation.

Recommendation 26 : Destruction of the card on the demand of the patient.

The patient must be informed of his right to require the destruction of his card and of how to exercise that right (letter to his doctor, to the host). By "destruction of the card is understood :

a) the rendering anonymous of all data stored at the service center relative to the issuing of the card and its contents. The host retains the right to make use of such anonymous data for scientific research ;

b) the interdiction to all medical personal to access or continue access to the data defined under a)

Recommendation 27 : Measures to be taken in case of loss or theft of the card

The patient whose card is lost or stolen must inform the host as soon as possible. The latter is held responsible to take, according to the procedures established at the time of delivery, every possible measure to render access to the card impossible. The center shall be held responsible for any abuse of the card taking place during the hours following the notification of loss or theft.

Recommendation 28 : Destruction of the card upon the patient's decease

Should the bearer of the card die, his heirs or any other person (e.g. his doctor) will demand the destruction of the card.

The card will be destroyed in the sense of recommendation 26 b upon notification of the host. The data shall be rendered anonymous one year after the bearer's death.

CONCLUSIONS

The medical data card (MDC) is undeniably a technical advance which could raise the quality of medical treatment. His development does, however, risk causing profound

changes in the relationship doctor / patient.

Traditionally this relationship consisted in the oral transmission by the patient of certain information, the culling of data from certain analyses and, finally, the oral transmission or by paper (protocols) by another doctor having had direct contact with the patient. Briefly, the patient controlled the sources of information.

The existence of centralized data banks renders more opaque to the patient the sources of information, but access to these is strictly controlled by the profession.

The card gives the patient, in appearance at least, the control of his own data, but, at the same time it puts in his hands a complete medical identity card. Where a doctor previously received partial information, he may henceforth, thanks to the card, have access to to the complete picture, certainly more reliable, but equally far beyond the specific necessity of his relationship with the patient. Furthermore,this information carried everywhere by the patient can multiply in numerous places and, once normalized, be susceptible to access by a multitude of persons.

Our aim is not to condemn an instrument of progress, but to strengthen its case with a certain number of guarantees the first of which is transparency : thoroughly informing the patient of his rights, evolve all the right to refuse the card, to know the nature of data it contains, the situations likely to develop around the use of the card.

The second is that of non-discrimination : it is important that the card neither limit the choice of a doctor nor be the cause of specific advantages pertaining only to users of the MDC system whether doctors or patients.

The third is the affirmation of limited finality of the card, conceived as a tool to assist the continuity of medical care and not as an instrument to enable the control of data by persons exterior to the relationship doctor / patient.

The fourth is the proper respect due to the principles of ethics in medicine and the laws of privacy on the part of all the intermediaries including the host.

Finally we would add that the highest standard of responsibility exercised by those entering information on the MDC is an indispensable condition for the reliability of the system.