The patient data card - Legal aspects - AIM Programme

Boulanger, Marie-Helene; Poullet, Yves

Publication date:
1990

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

6135

THE PATIENT DATA CARD

- Legal aspects-

AIM Programme

Professor Y. POULLET
Professor at the Law Faculty of Namur
(Belgium)
Director of the Centre de Recherches
Informatiques et Droit

M.-H. BOULANGER
Assistant at the CRID

We would like to thank here Doctor Karl Furmaniak for the precious help he gave us for this analysis. We also thank Professor André Bouckaert for his practically oriented contribution.

mars 90

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 and must therefore benefit from a specific protection.

In the first stage, we have tried to examine, from that point of view, the challenges raised by the introduction of a medical data card, then, in a second moment, we have looked at the existing applicable regulations and, finally, we tried to outline a new normative framework.

The Patient Data Card (P.D.C.) can be considered as a kind of 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 recourse 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 ; we talk about a card for medical professionals which will enable the same, under certains preconditions, to have access to the medical content of the P.D.C.. We are analyzing only the patient's card.

The advantages of the patient's PDC are primarily in the area of logic : the rapidity of treatment can be noticeably increased, particularly in cases of emergency. Furthermore, the patient benefits from a greater freedom in the choice of his physician 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 principal 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 areas :
- the violation of medical secrecy ;
- medical responsibility : reading the card may, according to certain authorities lead the physician 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 physician by the patient ;
- the liberty of the patient to communicate his card or not to different physicians participating in his treatment (guaranteeing his right of informational self-determination) ;
- the security, reliability and technical limits of the system and consequently the liability of his creators ;
- the risk of destruction or modification of the medical information, whether intended or not.

Finally, we want to give our discussion an European dimension even though the diversity of the public health systems make a common approach difficult. For example, the British National Health Systems is based on an asserted "ownership" of the medical data by the ministerial department of Health. It seems obvious that in that context, the setting up and the management of a PDC system will be the fact of the public sector perhaps compulsory and will countain administrative data. In a PDC system may be viewed on a different basis.

I. THE PATIENT DATA CARD AND THE QUESTIONS AT STAKE.

The questions at stake with the introduction of PDC are twofold: what are the contents of the card ? 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

'External contents' includes 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 of simultaneously being requested to present an identity card offers a better guarantee in this respect.

In case of loss or theft, such information permits the retrieval by the person concerned without recourse to technical means, thereby avoiding the reading of the internal contents. But one may ask, in order to exclude all risk, if it were not preferable to indicate on the card solely the institution responsible for its issue. In this manner, the card would be protected "from the curious" (see infra, Proposal 8).

B. Internal contents

"Internal contents" includes such data as can 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 presents itself, namely the necessity of finding a balance between a respect for individual liberties and
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 of such heterogeneous elements which were formally dispersed and includes the following :

- hospital records, or all information pertaining to the specific function of a hospital that provides health services (this data being under the responsibility of the hospital director)
- family physician's and specialist's records ;
- medical pass book ;
- administrative records.

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

The revolution in record keeping 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 PDC resides in the assembling of an individual dossier where can 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. First the administrative data, are inscribed on the card at the moment of issue and are usually not subject to modification. Second the medical data, are inscribed on the card at intervals as treatment progresses.

A. Administrative data

This category regroups 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]
Administrative data are used when admitting a patient to hospital or consultation.

It should be noted that the possibility of administrative data such as health care insurance, places of hospitalization, former admissions to a determinate service or that hospital, influencing the quality of care provided.

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

B. Patient data

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

By nature, the content is very varied. A first attempt to classification establishes a distinction of the medical data into two separate lists, distinguishing between objective and subjective data. For example, weight, age, sex, height may be considered as objective data. 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 physicians using there personal capacity for analysis may be considered as subjective data Such data may all be considered subjective to the degree that they require an interpretation on the part of the physician.

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.

---

[1]The newly draft bill in Belgium for the pretection 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.

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

Furthermore, it can be asked 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 other, as is the case, for example, with psychopathic conditions.

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

1.1.4. Distinction relative to target groups

One might think that an PDC 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 cards would justify a sufficient diffusion of scanners.

However, that may be , 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

Patient data cards are of interest to a certain number of category of persons. Each category has his specific preoccupations, first the users of the service (health care professionals-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 provider-patients

A. Card users

Card users are extremely varied. One may, however, distinguish between physicians, health professionals who are not physicians, and those whose work revolves around health professionals.

The members of the medical body would include the physician directly associated with the treatment or his replacement, general practitioner or specialist, the physician working in a hospital - more and more frequently part of a team - physicians working at home - individually or in association - medical biologists, insurance company physicians, company physicians, and the physician called upon as an expert witness...

Health professionals other than physicians such as chemists, physiotherapists and dentists would also be included.

Finally other personnel in the health care institution whose work revolves around health professionals are the amongst others hospital personnel, medical and paramedical personnel (whether in clinical or domestic services) and administrative personnel,...

The interests of health care workers are directly connected with the services rendered whether in treatment or on an emergency basis. In any way, 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 under the former system, physicians could limit the information longer in a position to know exactly to whom he is divulging the information he records on the card. Thus the physician loses a part of his control over the information.

B. Beneficiaries

Beneficiaries are those carrying the card, whether they are representative of the entire population or only a particular sub-group of the same.

Their main interest as health care consumers 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 physician. This facilitates the continuity of treatment and allows a patient to change physicians without difficulty.

Nevertheless, the use of the card is no neutral matter for the patient and leads to certain difficulties.

First and foremost, the patient may not necessarily wish the physician 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 the degree up where the physician may receive information concerning himself. In this way, the patient would seem to have to a certain degree to be assured of his right of informational self-determination or in other words to control the flow of information relating to himself.

Nonetheless, this assumption is relative when one places the relationship physician-patient in its context. Such a relationship is of the type "specialist-uninitiated" and may in reality illustrate a certain lack of equality. In practice, it would appear rather difficult for a patient to refuse his card to the physician 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, physicians, 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 logic system's base.

This can justify the will to reserve the management and the supervision of the PDC's for institutions controlled by the State or to public bodies responsible for the public health.

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 principal functions of such hosts, consist, on 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 a 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 lead, and , in a more general way, for its security and reliability. Furthermore, it is indispensable to achieve a certain normalization of hardware and software, if notably to free both physicians and patients from being bound for better or worse to one particular host.

1.2.3. Persons in periphery of this relationship

A Government authorities

The Government authorities are preoccupied with the politics of public health and the reduction of health costs. Do these preoccupations justify even the most limited access to the PDC and the keeping of a summary file of card holders ?

B Health insurance institutions

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

The aim of 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 PDC ? Wouldn't a reference to the paying institution sometimes present a danger with regard to the law of 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 will be very attentive to the impact of the system of PDC's on the medical practice. Let us mention, for example, the risk of discrimination between physicians owning a reading device and those who do not.

They may be enabled to play an important function in the matter of controlling the smooth functioning of the system and in the one that 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 they select a candidate for a job in order to know the state of health of the candidate employment and secondly, when they arrange the conditions of work with regard or in response to the health of the employee.

1current or future

E. Judicial authorities [1]

The data card can serve as evidence in private litigation or 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 inputs that are signed and dated, that it would help to determine the physical presence of a physician at a certain time and place. Finally, it seems likely to us that certain person could use it to determine the responsibility of a physician, this is in relation with professional misconduct or with prove negligence or fault connected to the use of the PDC system itself.

F. Institutions for medical research

Research institutions play a key function in improving the quality of health care, although they are not participating directly in treatment.

The information contained on the card may serve on one side for the purpose of medical research and on the other side for the control of populations considered at risk, or for disease prevention. The PDC system offers respecting 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 surveyed. Secondly, it represents treatment of data already processed and partially centralized by the host pertaining to an entire population or a large sample of right. The partial centralization realized by each host must remain partial to avoid a too great centralization in the research laboratory.

[1] civil and penal suits

II Existing regulations applicable to Patient Data Cards

The first part of our study attempted to define the principal areas of risk connected with the introduction of a PDC system. In this second part, we wish first to pinpoint the applicable regulation taking into account the general principles of the privacy laws and the professional secrecy and, secondly, taking into account the principles specifically applicable to medical data cards.

2.1. GENERAL PRINCIPLES.

2.1.1. General principles derived from the laws of privacy

The Convention of the Council of Europe of 28th January 1981 for the protection of individuals with regard to automatic processing of personal data states some general principles (accepted by the majority States of the Community) which seek to assure the protection of confidential data and thereby respect of privacy. We propose to analyze the different principles of this convention with regard to the PDCs.

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

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

B. Articles 5b et c prescribe respect for the principle of finality in the storage and use of data.

On the one hand, data should only be stored in proportion to the needs it serves. The only purposes permitted to justify the recording of data are relative to the admission or treatment of the patient. The storage 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 recorded, it is necessary to clearly delineate the finalities.

We can assume that the data is stored and transmitted in order to assure effective health care. More precisely, the data must facilitate the treatment of the patient -also in the 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 purposes other than these just mentioned (e. g. scientific research, supervision of the physicians) will be examined later.

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

C. 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 physician with respect to the conservation of

data. A patient who chooses not to present his card accepts as a consequence that it cannot be entirely up to date. Finally, the programmer is responsible for the conception and functioning of programmes.

D. In conformity with Article 5e, data may not be kept for longer than the period necessary to serve the legitimate goals of treatment. The question can be raised as to whether it is necessary to conserve medical data for a sufficiently long period.

E. Article 6 forbids the processing of various 'sensitive' data unless domestic law provides appropriate safeguards. Patient data fall into this category. provided the diversity of P.D.C. applications, statute law might not be the best solution.

Their collection and procession must be made in accordance with the principle of finality (see point A).

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

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

Firstly, it is not always desirable that the patient has direct access to the medical dossier on his PDC[2].Secondly, should it be possible that someone has an acces to his personal data contained in someone else PDC, as an example should a father have an access to his children PDC if a hereditary disease makes that he will be mentioned on the PDC. Even through the right of the patient be limited, he still retains the right to receive an intelligible summary of the same from his physician. This mediation offers certain advantages :

- the accessing of data takes place within the framework of a confidential relationship between physician and patient ;

- the communication of data is to a certain degree adapted to the patient inasmuch as diagnoses of a grave or fatal 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 of rectification. Such is notably the case if the rectification demanded is contrary to the observed medical situation.

Most of the national regulations drived from the Council of Europe Convention provides a compulsory centralized registration of all the data bases containing individual data. By example, the British Data Protection Act 1984 regulates the maintenance of personal information held on computers. The general medical practitioner computer system, the hospital systems and the one pharmacy system wich retains personal information are registered under the act for the purposes of the CARE Card Trial. The other pharmacy

---

1In Belgium, article 33 of the code of medical ethics requires the physician 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 France, according to article 6 of the law of January, 6, 1978, a doctor may choose that which he reveals to his patient, and according to article 42 of the code of medical ethics he is authorized to not say everything.

2In 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.

systems and the dental system do not retain personal information and do not require registration under the act. Whilst the CARE Card itself contains a microcomputer the data protection registrar advised that these did not require individual registrations since they were given to and belonged to the patients.

Registration includes details of the personal data held, the purpose for which it is used, the sources from which it is obtained and those to whom it may be disclosed. All authorised users "those to whom it may be disclosed" are covered by the Data Protection Act whether or not their particular system is registered. Failure to comply with the principles of the Act is an offence. All users agreed to comply with the Act and have signed the undertaking of confidentiality at appendix 1.

2.1.2. Professional secrecy

A. Principle

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

The obligation of secrecy reposes upon the privileged relationship established between physician 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 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 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 physician or any person holding secrets of state or secrets of 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 Belgian code of medical ethics obliges a physician 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 physicians in the interest of the patient within the conditions established by law. Article 378 of the penal code prescribes sanctions against physicians 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.

Under the british legal system, the law relating to confidentiality has also been the subject of several recent important court decisions form which clear legal principels have emerged. Medical information obtained from patients and matters relating to their health care and treatment are confidential, and may not be used for any other purpose; and the courts will import a legally enforceable obligation of confidentiality. A person or body infringing this obligation may also be in breach of copyright if such information is in a form which reproduces the whole or a subsantial part of material obtained from such a source.

The rule of secrecy in the patient - practitioner relationship has been built up and observed throughout the history of medicine. It was contained in early codes such as the Hippocratic Oath : "Whatever, in connection with my professional practice, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret".

B. Trustees of the secret

In order to be in conformity with this principle, the reading of medical information, must be confined solely to persons bound to silence.These are generally physicians and those

involved directly with treatment. In this latter group, there is a certain gradation of the obligation to secrecy under various national statutes.

The guidelines by which the health professions are governed have evolved over the years and all of the professional associations issue guidance on "Ethics and Legal Obligations". The guidance covers confidentiality issues and stresses that practitioners are responsible for ensuring that their staff observe strict adherence to these.

For certain professions such as 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 traditionally bound by the obligation of secrecy.

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

1. With regard to the patient

It is generally admitted that exists no obligation to keep information from the patient, on the contrary, the latter has a recognized right, to information although this right may be limited in certain cases, notably where knowledge of the diagnosis could have a detrimental effect on the physical or mental health of the patients (see above 2.1.1. G.).

2. With regard to the third parties

a) In general

It is clear and evident that exists an obligation of secrecy towards third parties. Information obtained in the course of consultation and treatment is confidential and personal health information, for the purposes of confidentiality, is indivisible. In other words, even such information as the fact that a patient attended on a certain day is part of the confidential record. No part of the record should in, normal circumstances, be disclosed by any user to any third party not concerned with the treatment of the patient. 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. Even the tacit authorization of the patient does not remove the obligation to secrecy. Indeed, 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 death of the patient.

b) Particular cases

- The public administration: the law enumerates and limits the cases where a secret can be divulged ;

- the courts : professional secrecy is not at the patient's disposal. The fact that the patient may have delivered his physician of the burden of secrecy does not oblige the latter to divulge, even in court, facts covered by medical secrecy .

- the 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 inside the health care team. It is also allowed between the hospital physician and the family physician.

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 THE PATIENT DATA CARDS

Before responding to the challenges posed by the card, we propose to review the norms specifically applicable in this domain. We shall open with the recommendations elaborated by the Council of Ministers of the European Council, n° R (81) 1 of 23rd January 1981 on the regulation for automated medical data banks and n° R (83° 10 of 23rd September 1983, on the protection of personal data used for scientific research and statistics. Afterwards we shall look at the essential principles delineated by the Commission Nationale Informatique et Libertés (C.N.I.L.) resulting from the experience gathered in France since the introduction of the PDC and at the Belgian experience in this matters.

2.2.1. Recommendation No. R (81) 1 adopted by the Committee of Ministers of the Council of Europe on 23rd January 1981, on Regulations for automated patient data banks

These regulations, although they are not constituting a normative statute in law, state important principles that the member States must respect when framing their national legislation.

The applicability of this Convention rests on two points :

1. the card represents a miniature automated data bank and
2. its purpose is clearly that of medical care.

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

The Recommendation delineates above all the necessity of subjecting any medical data bank to its own specific regulations, whose parameters are defined in the appendix to the Recommendation (A). It also expresses to promote awareness and information about the protection of medical data and treats of the principles relative to both recording and access to data (B and C) Finally, the explanatory report mentions the necessity of a major campaign of public information which would seem particularly desirable before introducing a system of Patient Data Card (D).

A. Regulation of data banks (point a of the Recommendation)

Specific regulations, established in conformity with the laws of the State concerned must comprise among other things, precise provisions as regards the following (article 3 of the appendix to the Recommendation):

- the specific purpose(s) of the data bank, categories of information recorded, the body or person for whom the data bank is operated and who is competent to decide which categories of data should be processed;

- categories of person who are entitled to record, modify or erase data;

- the parameters of access to the data bank and of the communication of information to third parties or individuals concerned and also the procedure relative to demands for the use of data for purposes other than those for which it was collected;

- the security of data and installations;

- the conditions under which, should the need arise, the data bank may be permitted to link with other data banks

Let us mention that separate supplementary regulations must be adapted to cases where the data bank contains several sets of medical records or sub-systems of medical data .

B. Recording of data

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

- collection by fair and legal means;
- the collection only of data adequate and appropriate to the declared purposes;
- the accuracy (verification within the limits of the possible) of the data and its actuality as appropriate.

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 physician. Keeping a medical record up to date is justified in the light of the necessity of continuity of treatment.

The text adds 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. (article 4.2 of the appendix to the Recommendation) . This obligation must be imposed on the designers and producers of cards. The files must also as a general rule be so designed as to enable the separation of identification data, administrative data, medical and social 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 (article 5 of the appendix to the Recommendation)

Primarily, access should be reserved, as a general rule, to medical staff. However, in conformity with national legislation, this access could be extended to other health care staff. In any case, no one should have access except to that information pertinent to the exercising of his specific duty , neither may he make use of that access for a purpose other than that for which he originally had access to those data.

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 , neither the existence nor the contents of a medical record may be communicated to third parties other than persons or bodies occupied in the fields of medical care, public health or medical research except in cases where the laws of professional secrecy permit it.

D. Public information campaign (article 2 of the appendix to the Recommendation)

The appendix to this Recommendation also underscores 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. Recommendation N° (83) 10 adopted by the Committee of Ministers of the Council of Europe on the 23rd September 1993, on Protection of personal data used for scientific research and statistics.

Lets note that the study of the Recommendation is relevant the personal data recorded on the PDC can, and probably will, be used for scientific research.

It recommends that the governments of member states take as their basis, in their domestic law and practice concerning the use of personal data for scientific and statistic, the principles and guidelines set out in the appendix to the appendix to the Recommendation.

The use of personal data for research purposes requires special protection measures in order assure a complete respect for the privacy.

Whenever possible, research should be undertaken with anonymous data (article 2.2. of the appendix to the Recommendation).Furthermore, the person furnishing data concerning himself should be adequately informed about :
- the nature of the project;
- the objectives of the project;
- the name of the person of body for whom the research is carried out
(article 3.1. of the appendix to the Recommendation).
Further, if the required information, given the purpose pursued, cannot be disclosed before the data are collected, the person should first be fully informed after the collection is completed and should be free to continue his co-operation or withdraw it and, therefore, be entitled to ask for the erasure of the data connected (article 3.3. of the appendix to the Recommendation).

On the other hand, the person from whom data are sought benefits from the freedom to provide the requested data or to withhold his co-operation ; anyway he is under no obligation to disclose any reason for his refusal to co-operate (article 3.2. of the appendix to the Recommendation).

The personal data obtained for research should be used for no purpose but research. In addition they should not be used to make any decision directly affecting the person concerned nor, as collected for the purpose of a given research project, they should not be used in connection with another project substantially different from the first one, except within the context of the research (in the first case) or with the consent of the person concerned (in both cases) (article 4 of the appendix to the Recommendation).

2.2.3. General principles of the Commission Nationale Informatiques et Libertés

At the time when opinions were given concerning experiments with cards, the French Commission Nationale Informatique et Libertés (C.N.I.L.) placed the accent more particularly on the following recommendations resulting from the lack of transparency of electronic memory cards. The following recommendations are particularly relevant as the issue has long been largely discussed in France.

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 PDCs on the practice of medicine, on the relationship physician/patient, on the application of medical secrecy and ethics.

Taking into account the respect necessity for the rights of the persons involved in the experiment delineated above :

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

2. Free and informed consent[1] to the use of the card. Patients and physicians 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 as reinforced by the restatement of that consent at each application of the DC system; the freedom of the patient 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 physician or patient.

Above all the introduction of a PDC system may not limit or restrain the patient in his choice of a physician [2].

Finally, a physician who participates in the PDC 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 physician and physician or physician and patient.

2.2.4. The Belgian experience.

We shall first sketch the experiment of the uniform medical "emergency card" set up by the Flemish Community and, afterwards, the advice formulated by National Council of the Order of the Belgian physicians. The Belgian Experience may be viewed as a good example both of an administrative approach of the PDC and of the reluctance of medical associations vis-à-vis the implementation of this new technology.

A. The uniform medical "emergency card".

In Belgium a uniform medical "emergency card" has been set up by the Flemish Community[3] with the purpose of standardization. The card consists usually of a in two fold "papier fort" but the use of a magnetic card may be allowed.
The following data may be recorded with the acknowledgment of the holder :
- the full identity of the holder ;
- the identification number ;
- some vital data which are of essential importance for a proper treatment of the holder (i.e. haemophilia)

1There must be a written consent according to the C.N.I.L.
2See article 27 of the Belgian code of medical ethic.
3Order of the Flemish Community d.d. 23 December 1986 setting up the uniform emergency medical card, M.B., 19 February 1987, at 2357.
Decree of the Flemish Executive d.d. 25 June 1987 for the enforcement of article 4 of the order of 23 December 1986 setting up the uniform card, M.B., 30 September 1987.

These last data are covered by the medical secrecy and must therefore be only read by the treating physician.

Are furthermore penally sanctioned :
- the unauthorized delivery of the card ;
- the delivery of a different card or its putting into circulation.

B. Advice of the "Conseil national de l'Ordre des médecins" (National Council of the Order of the Belgian physicians)

The Council of the Order[1] warned the public of the dangers inherent in the use of "Medicard", a Belgian PDC :
- dangers resulting from an abusive use of the card;
- the card may raise a false feeling of security (for the patient); the summary character of the data recorded on the card might lead to serious mistakes in the diagnosis; it is therefore of no great help in the treatment of the patient;
- the card consists of incomplete and out of date data with regard to the new clinical state of the patient.

The "Conseil National" pinpoints furthermore that the use of the "Medicard" may violate the patient's privacy as the thereon recorded data may be diverted from their original medical purpose.

The National Council has constantly reaffirmed its position.

1Advice of the "Conseil National de l'odre des médecins" about the "Médicard", d.d. 21 may 1980, Bulletin Officiel, N° 28, 1979-1980.

III. TOWARD A NEW NORMATIVE FRAMEWORK

Preliminary reflections

In the begin of debates about privacy, electronic data card has sometimes been considered as the solution to all the dangers that the computerization of our society presents for our personal liberties. It represents, at least in appearance, a reappropriation by the individual of information concerning his own person : the individual would finally retrieve control of whether to communicate or not the image of himself given by the data on the card to others. Some go so far as to say that through the electronic card a person becomes again the owner of his own data.

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

a) the written data is reproduced somewhere else :

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

c) in comparison with data banks constituted outside the control of the individual, the access to the data bank, frequently compartmental, is rigidly controlled by the director of files while the electronic data card risks create a major risk to give an access to the complete dossier, to readers of who now could put pressure on the bearer;

d) in that perspective not only newly inscribed data would 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 could 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 PDC, but rather to underline the importance of a regulatory framework capable of reducing the risks created by this new technology and of reinforcing interests in this alternative to centralized data banks. In that perspective, we have put some proposals or, rather, different themas whereabout further regulatory or self regulatory measures must be kept. Mainly it is asked taht on those themas, further reflections are developed in the context of the AIM PDC W.G. follow-up. It is obvious taht the list of themas is not complete. Other themas have been identified by the PDC W.G. as the question of the delivery of cards to children, the possible mixture in a same card of the reimbursement function and the continuity of care function, the prolbem of the inclusion in the card of informations pertaining to third parties...

The presentation of our proposals relative to this framework follows a chronological plan :

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

3.1. SETTING UP OF A SYSTEM TO PROCESS PDCS

The choice of a system supposes as previously stated a number of important technical questions.Their importance is considerable since they condition the safeguarding of the confidentiality of the data involved. Without being exhaustive, the following aspects should be considered :

- the type of PDC : according to the technology chosen, the capacity of the cards may differ appreciably. The distinction of separate zones of access 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 physicians 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 utilization of the PDC;

- 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 system and the host 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 authorize the physician 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 PDC at the expire of a fixed period or upon loss of the card;

- the eventual rendering anonymous, within the framework 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 proposals seem to us to be appropriate to the introduction of a system for processing PDCs. Certain of them are directly taken from the Proposals of the European Council, 23rd January 1981, relating to medical data banks (see above, n° 2.2.1.).

Provided the diversity of the PDC's applications, "hard law" regulatory instruments would not be appropriate. Let's insist on the fact that a self-regulation is preferable. We shall therefore limit our discussion to a number of proposals.

Proposal 1 : Principle of self-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), the security measures taken to assure the confidentiality of the card, and

finally, the processing measures necessary to assure respect for medical ethics (e. g. within the host, access to medical data would be reserved solely to health professionals bound to professional secrecy).

Proposal 2 : Principle of nomination of a responsible for every processing system

The person would supervise the application of the principles relating to the privacy laws when issuing the medical cards and during their circulation. Further he would be responsible for the respect of the rules governing the rights of access.

Proposal 3 : 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 for questions of data protection. This double control should take place not only at the system's conception but throughout its period of service and particularly in event of modification.

Proposal 4 : Principle of publicity prior to the existence and development of PDC processing systems

Parallel to the Proposal already made by the Council of Europe for automated medical 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 information would permit those in interested parties to make their point of view known before significant levels of investment have been reached (see above, n° 2.2.1.).

Proposal 5 : Principle of card structure

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 separate section for emergency data (on the meaning of this category, see infra, Proposal 10)

3.2. DELIVERY OF THE CARD TO THE PATIENT

Two questions must be asked.

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

Without wishing to quash 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 responsibilities of security and confidentiality.

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

The respect of these principles justifies the following proposals :

Proposal 6 : Principle of patient information thoroughly prior to issuing the PDC

The information of the patient must be broadly conceived not only with regard to the purpose, nature and modus operandum of the system, the contents of the card (nature of data stored), the individuals authorized to read or record data , the procedure to follow in event of loss either of the card or of one's personal code number (Personal Identification 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.

Proposal 7 : Principle of free consent to the issuing of the card

This proposal seems to us to have two meanings: firstly the delivery of the card may not be either directly or indirectly, construed in any way as a condition of access to medical services; the second makes clear that a document explaining the essential information delineated above in proposal number 6 should be submitted in duplicate to the patient for communication, consent and signature with one copy of the document to be retained by him.

3.3. THE CONTENT OF THE PDC

Our introduction distinguished 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. Obviously, the external content of the card must be kept to a minimum. 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, including someone close, might identify the bearer and endeavor to read the contents. Proposal 8 may be therefore framed as follows :

Proposal 8 : Principle of minimal set of data on the PDC exterior

Following the opinion of certain people, preferably the exterior of the card should 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.

This solution will persuit that in case of loss or theft, it will be difficult to identify the card drawer except if you have an access to a reading divice machine.

Other people point out that the anonymity of the PDC exterior makes impossible a control by the physician of the identity of the drawer and so will be dangerous so far an illegitimate drawer can ask for having access to the internal content of the PDC.

As regards the exterior content, it will very following the national regulations. For example, in certain countries, the appartenance to a health Insqurance company is viewed as a sensitive data.

This definition is one of the most difficult point around the PDC system.

A first definition can be the list of what the E.E.C. recommandation about the emergency medical card includes as emergency data. This list is very limited because the purpose of the E.E.C. recommandation was to propose a minimal set of medical data largely accessible.

If we chose that definition, the emergency data may be accessible with the same level of security that administrative data. But if we accept a broader definition, e.g. any data that will help unconscious patient or still broader, any data that will help a doctor unfamiliar to the patient to diagnose and treat in an acute illness, the access to emergency data must reserved to health professionnals, excluding ancillary of administrative staff.

Provided of the interest of this second approach, we propose the following thinkings.

The second criterion concerns the type of files kept by the card. Proposal 5 proposed already the structuring of the card. Beyond that, should one limit the number or type of dossiers held ? Without going into questions of memory capacity, a priori, one must recognize that every type of medical file, inasmuch as it merits being kept 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 pregnancy of a surgical nature, having no further history).

In the respect of the content, 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 the inclusion of this or that dossier, except at one opinion 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 physician inclined to rely on the information given by the PDC.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 patient to have certain emergency indications recorded on the card, for example drug dependence or AIDS, must result in the withdrawal of the card.

Proposal 9 : 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, reservation of subject to the proposal 10.

Proposal 10 : Definition of emergency data and regulations pertaining thereto

Under "emergency data" are included only informations whose ignorance on the part of the physician could have a gravely prejudicial effect upon the health of the patient.

Emergency data must be separately accessible. They must be accurate, up to date and as complete as possible. Furthermore, a standardization of the data is absolutely necessary.

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

Finally, the notion of administrative data accessible to ancillary staff must be clarified. If one gives the PDC a finality purely connected to the continuity of treatment , the inclusion among administrative data of, for example, regular stays 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 proposals are general. Regardless of which health care professional is authorized, it seems important to us that the issuing of an personal identification number (PIN) for reading or inscribing should follow strict regulations. These regulations are the object of the following recommendations :

Proposal 11 : Principle of liberty

This principle echoes proposal 7. No health care professional may be forced either directly or indirectly to participate in the introduction and use of a PDC system. No discrimination whatsoever may result from a refusal of the same (see n° 2.2.3.).

It is ovious that a legislation can decide differently. So, a public National Health System (N.H.S.) can impose to all health card professionals involved in the N.H.S., to use the PDC in any case for administrative purposes.

If the use of PDC is mandatory, two problems must be adressed :

- the absolute distinction between the medical dossier and the administrative record in order to maintain eventually the principle of liberty to the medical dossier;
- the need of a regulatory environment to ensure the confidentiality of the medical data.

Proposal 12 : Principle 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.

Proposal 13 : Principle of ethical monitoring of authorization

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 place such measure as 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 physicians* . 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 physician, etc, would appear acceptable, the issue of access to medical data, as it is asserted by the Council of Europe proposals emergency data, is debatable. The principle at issue is that, even in the case of central data banks, access for paramedical personnel may be allowed through the intermediary of a physician 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 PDC.

Within the medical profession itself one may question the right to access of certain physicians. 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 physicians 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 physician entrusted by the bearer with access.

Indeed it would seem to us, that the requirement to present the PDC 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, the continuity of health care, in a more safe and effective manner.

This goal would however justify reading access to all medical personnel directly involved in treatment (whether or not they are in training).

---

* In certain countries, other Health care professionals are submitted to the same professional duties and secrecy than the physician, for example the chirurgical dentists in U.K. and must therefore benefit of the same acces than the physician.

Proposal 14 : 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 PDC 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.

Proposal 15 : Principle of refusal of the use of the card for purposes other than the stated finality of continuity of health care

Without prejudice to the questions inherent in epidemiological research, the physician, 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 the patient's health ;
- provide expertise for private litigation or criminal prosecution ;
- ...

3.4.2. The actual reading access

The problem of reading access is a dual one : on the one hand, it is the determination of procedures to permit a physician to have access to the contents (a) and on the other hand the right of the patient to have access to data concerning himself (b).

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

Proposal 16 : Principle of patient authorization for reading access

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 identification number (in the case of minors this is the function of parents).

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

With regard to the physician, in that which concerns his right to copy data from PDCs, 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 a 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 precedent conditions relative to medical secrecy with regard to the patient lead us to make the following proposal.

Proposal 17 : Right of the patient to read his own file

If an institution (e. g. a hospital or practicioner) has a reading device for the PDC, 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 physician of the institution. The institution should have the right to limit the information to a summary by the physician. 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).

In addition, the right of access of the patient should not be diverted from its original purpose to allow an unauthorized third party to get access to the information.

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- (see proposal n°10) It seems to us that the affirmation of this right of the patient would facilitate the social acceptance of the card.

Proposal 18 : 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 practitioner will determine if the erasure of the information is detrimental to future medical treatment (see proposal n° 10).

It is abvious that the erasure of data concerns only the information entered on the data card. It is the duty of the doctor to keep the data on other supports (paper or data bases).

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 its presence increase the responsibility of anyone entering data.

Certain proposals seem to us to impose themselves :

Proposal 19 : Principle of possibility for any physician with access to be able to enter data on the card 'directly or indirectly)

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

Proposal 20 : Principle of physician's right to correct, complete or bring the card up-to-date

Should medical examination suggest that certain data is incomplete, incorrect, or not up-to-date, the physician shall reserve the right, after having checked his own findings, of correcting, completing or bringing the patient's card up-to-date. In order to prevent errors and, eventually, problems of liability any conections, updatings must lead to the diletion of the previous informations.

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

Proposal 21 : Principle of data entry signature

All data entry on the card must be accompanied by the "signature" of the person responsible for the entry.

It is clear that this proposal 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. Proposal 22 attenuates this as follows :

Proposal 22 : 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 physician, who has placed reliance on that information, from his responsibility[1]. The physician has the duty, within reasonable limits, to make the necessary investigation to ascertain the accuracy of data on the card. In particular, the physician 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 modification is not possible 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.

Proposal 23 : Principle of introduction the renewal procedures

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

Note that the same rule should apply where data must regenerated as the result of accidental erasure 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.

With regard to the first question it is easy to reply that it is up to the physician 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 (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

1See article 2 of the french law "Informatiques et Libertés", 6 January 1978

time the cards has been 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 or genetic disorders where it is necessary to conserve detailed 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 epidemiological research was raised in our discussion on the areas of risk arising from the PDC 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 proposal should be made :

Proposal 24 : Principle of conservation of data

If the host intends conserving data beyond the limit necessary for the continuity of treatment, it must supply a motive for that conservation (e.g. scientific research) , assure the anonymity of data thus conserved, and inform the patient thereof;

The latter must be able to refuse 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 physician with access to the card may be envisaged in two ways. A first hypothesis is that the physician 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 proposals are useful :

Proposal 25: Relationship between physician and host at the time of issuing the card

The patient must be informed of all possibility of communication between physician and host.

The host 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 host 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 physician 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 between hosts are planned between hosts a regulation should 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 hosts.

3.6.2. The problem of destruction of the card.

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

Each of these cases should be the subject of a proposal.

Proposal 26: Principle of destruction of the card upon patient request

The patient must be informed of the right to require the destruction of the card and of how to exercise that right (letter to the physician, 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 and the physician the duty to keep the informations on other supports;

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

Proposal 27 :Principle of loss and theft protection

The patient whose card is lost or stolen must inform the host as soon as possible. The latter is responsible for taking 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.

Proposal 28 : Principle of the destruction upon death

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

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

CONCLUSIONS

The patient data card (PDC) is undeniably a technical advance which could raise the quality of medical treatment. Its development does, however, risk causing profound changes in the physician/ patient relationship

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 physician having had direct contact with the patient. Briefly, the patient controlled the sources of information.

Through his general pratitionner, 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 physician previously received partial information, henceforth, thanks to the card, 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 be increased in different locations 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 : the right to refuse the card, to know the nature of data it contains and to be aware 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 physician nor be the cause of specific advantages pertaining only to users of the PDC system whether physicians 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 physician / patient.

The fourth is the proper respect due to the principles of ethics in medicine and to the laws of privacy on the part of all the intermediaries including the host, not necessary aware of these principles. Further, one should care for the extension of the ethical principles to the new actors, even outside of the health care sector.

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