CPME/AD/EC/070707/116/EN

At the CPME Executive Committee Meeting, Brussels, 7 July 2007, CPME adopted the following document **"CPME Response concerning the working document on the processing of personal data relating to health in electronic health records (EHR)[1] - Article 29 Data Protection Working Party"** (CPME 2007/116 EN)

Concerns the Working document on the processing of personal data relating to health in electronic health records (EHR)[2]

Article 29 Data Protection Working Party

CPME RESPONSE

1. INTRODUCTION

As the consequences of data protection in relationship with emerging e-health technology will revolutionize their way of practicing, physicians should be heard on this subject and should be participating in the conceptual developments. Therefore CPME wishes to participate in this very important thought process in the interest of patients and its members alike.

Directive 95/46/EC outlines a few basic principles on data protection we can without reserve adhere to, but we also think that this directive needs a more detailed interpretation on recent developments in the e-health context and that more detailed rulings, specific for the health-care sector, are more than necessary.

It has become increasingly clear today that all forms of e-health have become an integral part of both physician and hospital work. It has facilitated existing processes and it has created new opportunities thus leading to a general acceptance in the profession.

E-health should facilitate existing work schemes and communication flows thus improving patient safety and quality of care. E-health should not sacrifice the existing well functioning model of the patient-doctor relationship.

[1] WP 131
[2] WP 131

The patient-doctor relationship implies a direct and physical, face to face contact between the physician and his patient. This particular relationship is not only built on mutual trust but also on human communication skills and observation. All physicians agree that a direct anamnesis and physical examination of the patient is the cornerstone of medical practice. This can not be replaced by robotised, virtual or remote procedures.

These procedures can be used however when under very specific circumstances direct contact can not be established or is very difficult to be established.

CPME strongly calls for the consideration of new risk scenarios. The more data is concentrated and aggregated the more attractive it becomes for a whole lot of potential power players.

Paper records only exist in one place at one time and can only be copied in a cumbersome procedure. EHRs give a totally new dimension to the security threat and should also induce a totally new reflection on the optimal protection.

CPME wishes to stress the importance of a European-wide regulation of identification and authentication procedures for patients and health care professionals alike. This regulation is a prerequisite for any form of integrated E-health applications. Also, a legal framework should be in place before the further development of e-systems in order to provide the legal safeguards needed.

2. DEFINITION OF EHR

"A comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form and providing for ready availability of these data for medical treatment and other closely related purposes"

CPME agrees that such an ideal record will improve quality of care and provide important data for planning, statistics and quality control in health care.

Currently though, the form and content of medical records varies tremendously in the different member states due to ethno-cultural, historical and system reasons. CPME draws attention to the fact that the implementation of e-health and EHR solutions in different countries has already come a long way without any consideration for integrated trans-border approaches. It is important that further developments take account of the increased migration of patients and physicians.

Depending on whether countries have oriented their systems to more or less centralised data-bases and storage solutions, health care records exist under different shapes. We do not know of systems which integrate all available data on a patient in a commonly accessible single record. Usually medical records are

individual data compilations on a given patient gathered by a specific institution or health care professional.

Standardisation, modular structures, common data modules, patient summaries and resumes are extremely difficult to realise and create a totally new set of yet unknown problems on issues such as updating, liability and validation. These concepts need to be discussed in-depth and thoroughly tested with the full involvement of physicians and other health care professionals.

3. DETAILED COMMENTS

All data contained in medical documentation, in electronic health records and in EHR systems should be considered to be "sensitive personal data"

CPME agrees.

Consent must be given freely
Consent must be specific
Consent must be informed

CPME agrees to these basic principles which imply that patients' consent should never be taken for granted or be obtained on a simple declaration of intent.

In emergency situations "break the glass" procedures should be made possible. This should only be possible if a relevant legal framework and adequate logging procedures are in place.

This relationship of confidentiality (patient-doctor) excludes all third parties, even other health care professionals, unless the patient has agreed to passing on his data or it is foreseen especially by law

CPME regards this to be a general principle.

Keeping and using patient's records is traditionally limited to the direct bilateral relationship between a patient and the health care professional

CPME agrees.

The article 29 Working Party is not convinced that relying only on the obligation to professional secrecy provides sufficient protection in an EHR environment. A new risk scenario calls for additional and possible new safeguards beyond those required by Article 8 in order to provide for adequate protection of personal data in an EHR context.

CPME agrees and supports your call for enhanced protection.

3.1 On self-determination:

After submitting this chapter to our members it has become clear that concepts vary widely. Some countries allow for opt-outs or partial opt-outs in relation to consent for the recording and/or sharing of health data. In particular, the Scandinavian countries do not accept opt-outs or give the patient a right to erase or delete part of their records. They do give them total access and the right to include personal entries in

the records. Other countries give the patient the right to modify or delete part of their records. In France they might not even allow for a "flag" to indicate that there are deleted portions in the record.

Patient rights in certain member states may extend to the ability to conceal or erase parts of his/her record. If this is done, it is in the interests of patient safety that there is an electronic "flag" on the record to indicate this. It is also important that patients are fully and comprehensively informed about the possible risks to their care by suppressing a part of their medical record. Issues such as physician liability and the patient responsibility in this context require special attention.

Access to the records is regulated differently from country to country and this may prove to be problematic, particularly on the level of third party data and certain highly sensitive (i.e. psychiatric) data.

The degree to which the extent of disclosure of data to other health professionals is granted varies as well. Again, Scandinavian countries accept a wide definition of sharing data among health care professionals. Other countries might require specific consent by the patient for every single data transfer.

CPME considers it good practice for patients to be asked for consent to the recording and/or sharing of data. CPME recognises that different member States and systems have varying approaches to these processes, but in *general* terms:

- Although consent can be presumed for the recording and sharing of information required for healthcare within the immediate healthcare team, it is good practice to obtain specific consent for this process, particularly in relation to sensitive information
- Specific consent should be obtained for the creation of a summary healthcare record, as well as for the sharing of information beyond the healthcare team

CPME recommends that in all cases and regardless of access control, an appropriate legal framework and relevant logging procedures should be in place to protect and regulate confidentiality.

3.2 On Identification and authentication

Health cards on smart card basis could contribute significantly to a proper electronic identification of patients and also to their authentication.

CPME recognises the advantages of systems based on both patient and physician cards. We do however note that certain countries have developed alternative means of identification and authentication, including measures to ensure the secure transmission of data.

In cases where cards are used both of them should be smart cards, not contain any direct data and should be used together and simultaneously to gain access to patient data. They should also include digital signatures and encryption capabilities.

Proper identification and authentication are essential, without these the whole system cannot work. Therefore CPME considers this to be a priority.
Also systems used to identify and authenticate must be compatible to service the increased migration of both patients and physicians.

General requirements of these systems are:

- Reliable confirmation of the physicians qualifications and registration/licensing status needs to be established in relation to the validation of the identity of the physician

- Clinical data should be accessible only with the consent and the identification of the patient, to the nominated physician.

Only those healthcare professionals/authorized personnel of healthcare institutions who presently are involved in the patient's treatment may have access. There must be a relationship of actual and current treatment between the patient and the healthcare professional wanting access to his EHR record.

In most of the countries the access to the record is limited to designated health care professionals who are directly involved in the patient's treatment/care and CPME is supportive of this approach.

Accessing medical data in an EHR for purposes other than those mentioned in Article 8 should be in principle prohibited (insurance companies, employers, institutions for granting retirement et al)

CPME agrees to this and stresses the need for a legal framework so infringements of these rules can be punished. In order to enforce this concept during identification and authorisation of the health care professional it should be mandatory to identify the status of the physician under which the data are accessed.

All information made available to healthcare insurers (whether private or governmental) must be restricted to the level required for the validation of a claim for payment or reimbursement.

3.3 On organised structure of an EHR system

Decentralised storage
Centralised storage
e-service under the patient's control

Although CPME generally is of the opinion that patient data should be stored as close as possible to the location in which they are created, we recognise that conflicting arguments exist about the security, vulnerability and accessibility of both decentralised and centralised databanks.

In all cases of data storage, however and wherever this takes place, there must be clear and enforceable rules on how data are accessed and by whom. It is a requirement that all those who access data demonstrate a legitimate reason and mandate for doing so. Authorities with responsibility for storing personal health information should have relevant certification and should be submitted to relevant auditing procedures.

Categories of data stored in EHR and modes of their presentation

a) Completeness

For CPME completeness of data is a basic requirement. Any data might be relevant at one time or another and relevance can not be foreseen.
Resumes, as said before, pose problems of update, liability and responsibility.

b) Presentation of data (data modules)

The creation of special data modules is not desirable as it is not possible to pre-define a specific need of data use for a specific category of users.

c) Special access

CPME strongly opposes any access to the EHR by third parties. Specific information can be transmitted on request and by authorisation but never by direct access.

3.4 On privacy enhancing technologies

Privacy enhancing technologies are a prerequisite. CPME agrees with the Working Party's statement that all the costs involved to implement what has been described in this document should not be seen as a financial burden or a budgetary constraint but rather as an investment in the future. Without this commitment you lose the trust of the users (physicians and patients alike) in the system and the original purpose will be lost: the gain in quality and patient safety.