COMITÉ PERMANENT DES MÉDECINS EUROPÉENS
STANDING COMMITTEE OF EUROPEAN DOCTORS

CPME/AD/Brd/191007/132/EN

At the CPME Board meeting, Brussels, 19 October 2007, CPME adopted the following document **"E-health – CPME policy statement on electronic health records"** (CPME 2006/132 FINAL EN)

E-health – CPME policy statement on electronic health records[1]

Introduction

Because of the growing importance of e-Health technology in the delivery of healthcare, CPME strongly values its use in supporting the physician in his/her work.

In discussion among the medical associations of the EU members States, it is clear that considerable differences exist in the approach physicians adopt towards e-health, based on differing application of ethical principles, the degree of patient control over the record, and the level of integration of e-health solutions in healthcare systems.

Because of these differences, CPME can set out some essential principles regarding the use and development of e-health systems, but we also stress that further study and development is needed to establish how to address the different approaches, both technical and ethical, that exist, as they currently offer a considerable barrier to the concept of an EU-wide system.

Our principles are derived from established practice across the EU, developed on the basis of paper records. Both paper and electronic records should serve the same basic purpose, which is to provide optimal care based on face to face contact and trust between the patient and the physician. This face to face contact is the cornerstone of the patient-physician relationship. With this in mind, the main objective of e-health technology must be to ensure and support quality of care and patient safety provided by health-care professionals, in full respect of current ethical and legal principles.

[1] The CPME defines the Electronic Health Record as a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual and the medical procedures done in electronic form and providing for ready availability of these data for medical purposes.

Rue Guimard 15 - B-1040 Brussels - Belgium
Tel. : +32 (0)2 732 72 02 - Fax : +32 (0)2 732 73 44 - E-mail : secretariat@cpme.eu - Web : http://www.cpme.eu

CPME cannot emphasise too strongly that it is essential, in order for this tool to be fully effective, that physicians are involved at all stages in its development. Acceptance by physicians and patients can only be achieved if the technical, financial, educational, structural and ethical issues as well as issues relating to information governance are properly thought through, and are reflected in the design of systems, which will require collaborative effort. Too often the development of hardware, software and networks has preceded consideration of the environment in which they will operate or has been derived from other professional frameworks. This is entirely the wrong approach.

CPME recognizes that there is a tension between the need for interoperability of healthcare technology (reflecting the mobility of patients and doctors across the EU) and significant national and local differences in e-health applications. Therefore CPME urges the close engagement with the profession and patients at all stages of development.

Main principles

The cornerstone of the physician-patient relationship is the face to face contact between them. The developers and designers of E-health applications should keep in mind that these applications need to support and enhance this contact.

Because of the privacy and trust inherent in the patient-physician relationship, security and confidentiality of systems are of paramount importance.

Security and confidentiality must be guaranteed and delivered by secure and reliable identification and authentication of both the patient and the healthcare professional.

Transmission of data has to be confidential, secure and purpose-related.

The absolute respect of medical confidentiality is of utmost importance in all e-health applications. To ensure this, systems must have:

- secure and encrypted paths of transmission
- defined messaging standards
- systems for acknowledging message reception and reading so that the sender can be sure the transmission is successful.
- logging procedures
- reliable identification and authentication procedures

The content of messages should be suited to the specific purpose in all communications regarding information between institutions or healthcare professionals. Online exchange of patient information between care providers should follow a standardised format in the interests of clarity and patient safety.

Although CPME has previously set out the preconditions for the development of a European card for health care professionals and for patients, we recognise that practice in some member States has shown that other solutions can guarantee an

equal standard of security. (For previous CPME work in this area, see CPME 2004/025 Final)

However, systems used to identify and authenticate must be compatible, to reflect the increased migration of both patients and physicians.

General requirements of these systems are

- In relation to validation of the identity of physicians, reliable confirmation of the physicians qualifications and registration/licensing status

- In relation to the identification of patients, any clinical data held should be accessible only to the nominated physician, and with the consent of the patient. Information made available to healthcare insurers (whether private or governmental) must be restricted to the level required as defined by the physician for the validation of a claim for payment or reimbursement.

Although a medical record will be held by a physician or healthcare provider, it must always be remembered that the ownership of personal *information* (in contrast to the record in which it is held) remains with the data subject, in this case the patient. This is an important ethical principle, which overrides considerations of the physical media and location in which the data is actually held or stored. Where patients have significant ownership of, or control over their medical *records*, they should also hold the "key" to the data, such as an electronic card or other technical method (e.g. a PIN code)

It is 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

Information collected and used for research or epidemiological studies must be anonymised (if specific and informed consent has not been obtained).

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 and the legal protection of both patients and physicians that there is an electronic "flag" on the record to indicate this. It is also important that patients are fully and comprehensibly informed about the possible risks to their care by suppressing a part of their medical record.

In emergency situations, physicians should be able to access a record, if they consider this to be in the best interest of the patient, providing that:

- the access is logged, and an audit trail is created
- the access is disclosed and explained as soon as possible to the patient
- systems establish an ombudsman/network supervisor/data controller process to oversee and monitor access
- a relevant legal framework is set in place

Although CPME generally believes 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. It has to be guaranteed that organisations storing health data have no interest in using this information for any other purposes.

CPME welcomes e-prescribing and medication records as a tool to improve patient safety. A recent survey carried out in CPME member states showed that e-prescribing is widely accepted and used in Sweden, Denmark and The Netherlands.

<u>Further consideration</u>

In addition to the essential principles listed above, CPME recommends that further investigation, in close association with physicians and patients, is carried out on:

- The controls that should exist to secure personal medical information held in databanks, whether local or central

- The challenge of building both flexibility and compatibility into systems to reflect the considerable differences towards consent and the sharing and disclosure of both identifiable and anonymised health data, that currently operate across the EU

- Issues around the rights of patients of access to their data, how third-party data is protected, and in what circumstances patients should be able to change factual information about them

- The impact of e-health on society, including the use of technology to improve information to patients, to more fully enable them to share in the management of their condition

- The impact of technology on the working patterns and environment of healthcare staff, and on teamwork
- The effective transition or adjustment of health care staff using such technologies
- The impact of e-health on workplace efficiency
- The impact of e-health on quality care or treatment
- The development of appropriate solutions to allow equality of access to e-health tools for young people and those with reduced capacity
- The size of the budget devoted to costly IT solutions, and the potential constraints on the healthcare system as a whole

Rue Guimard 15 - B-1040 Brussels - Belgium
Tel. : +32 (0)2 732 72 02 - Fax : +32 (0)2 732 73 44 - E-mail : secretariat@cpme.eu - Web : http://www.cpme.eu