



CPME/AD/Brd/251008/181/EN

At the CPME Board Meeting, in London, United Kingdom, on 25 October 2008, CPME adopted the following document : “E-health – Consent and Confidentiality” (referring to CPME 2008/181 Final EN)

E-health – Consent and Confidentiality

Confidentiality of patient data is crucial for physicians and other health care providers in order to conduct their work in accordance with the requirements of professional responsibility and diligent care. All patients, irrespective of background and the nature of their problem should be able to seek medical assistance being confident that their sensitive personal data can only be accessed by health personnel involved in their care. If the patients do not trust that confidentiality will be maintained, they might withhold medically essential information.

Nowadays, personal health data are collected, processed and stored electronically. This may improve data quality, sharing of information, accessibility to important information, and quality and efficiency of care. However, electronic patient records make it easy to obtain unlimited access to information if security systems are not good enough. The challenge is to make sure that only health personnel directly involved in the patient's care have access to patient records and other personnel information about the patient. Such information must only be accessible to health care personnel who need this information to provide appropriate care. Hospitals and other health care providers should be obliged to have an effective security system. These systems must guarantee the appropriate level of availability and secure storage of information. The patient will have limited control of what kind of information is entered into the record. To be treated by health personnel also implies consent to documentation of health information.

Main principles:

- Confidentiality must be maintained. Patients need to have trust in doctors and health care systems so that the best possible care can be provided.
- Patients should be able to obtain a copy of all or part of their medical record and ask to have factual errors corrected. Such corrections have to be visible to users of the records.
- Information must be securely stored and protected from unauthorised access.
- Authorisation rules must ensure that access is only obtained by medical or nursing staff that need to have the information for the care of the patient.
- Information for purpose of consultation and education should be made anonymous if not jeopardizing the safety of treatment.
- A full audit trail should be kept of every attempt, whether successful or failed,



- The patient must be able to confine access to parts of the record, e.g. psychiatric reports, to a limited group of health personnel.
- Transfer of information or extending online access to new health personnel involved in the diagnosis or treatment requires the patient's consent.
- There should be strict limitations on transfer of medical records to institutions outside the health care service. As a main principle, insurance companies should not be allowed to request the medical record or parts thereof.

Summary Care Record – consent and confidentiality

Many European countries are currently working to find solutions on issues related to electronic patient records. One option that has been discussed is to create a summary care record (SCR), which can be accessed online on certain conditions. The summary care record should only contain an extract of the patient's full medical record, and the information may only be uploaded if the patient gives consent.

It is a prerequisite that informed explicit consent will be necessary before a SCR is established, but it is not clear what will happen if wider sharing of the data is needed. CPME's opinion is that the patient should be contacted to give explicit consent to extended use of the data. It will weaken the individual's control of the data if implied consent is possible for wider sharing. A system for obtaining informed and explicit consent when the conditions for the SCR are changed must be established.

Another issue related to consent is vulnerable groups, for example people who do not speak the national language or have limited understanding of SCR. The national health authorities must take the responsibility to ensure that all population groups are fully informed about the consequences of establishing a SCR.

Each time the patient uses the health service; new information will be added by different health care personnel, perhaps with conflicting views on treatment. There will be a need for an overall quality assurance system to secure that the information in the SCR is correct, that differences in evaluation of health care needed is clearly marked and that the kind of information entered into the system is clearly defined (from whom and where it comes from).

The medical benefit of SCR for the patient can be questioned. If quality control systems are not established health care personnel can not fully trust that they have the correct information to make a proper evaluation and conclusion about the patient's health problem.

The medical record is the patient's property (this varies between countries), and must be respected and protected. Only health personnel involved in the treatment of the patient should have access to the SCR. But we know from other registers, for example account information systems in banks, that it is almost impossible to establish systems that can not be abused, either by individuals, groups or a totalitarian government .

We live in a society where it is tempting for the authorities to merge information from various electronic registers in order to obtain information on people's health and behaviour, e.g. on people who receive benefits from the social security system. It is



important that the access to merge health information with other registers is strictly regulated.

Patient created medical records

Google has launched Google Health, a free service for patients offering a personal electronic medical record (www.google.com/health). This is a new development where people may choose to distribute information on their health on their own initiative. An individual will be able to create an account, protected by a password, and enter personal medical records, either by keying them in or by importing electronic records from hospitals, laboratories, and pharmacies that are Google Health partners. It is difficult to foresee all the consequences of such systems, but they will probably not be as secure as public systems. A widespread use of such systems may have as a consequence that those who have access to computers and are familiar with their use may have easier access to health care providers. Another problem is that many patients may not be able to discriminate between basic health information and more sensitive information like information about hereditary diseases. EHealth is mainly market and technology driven. This implies that electronic medical records can become an interesting and profitable business opportunity for internet companies.