International Working Group
on Data Protection
in Telecommunications

675.32.27

Working Paper
on
Online Availability of Electronic Health Records

39th meeting, 6-7 April 2006
Washington D.C.

The Working Party has highlighted the growing importance of web-based telemedicine earlier[1]. The availability of electronic health records in networks (in particular the Internet) throughout a patient's life and beyond poses complex additional questions. This online availability of electronic health records is favoured mainly on the following grounds:

- lower costs for processing medical data,
- the immediate, "ubiquitous" and (seemingly) complete availability of the data
  - for doctors to benefit the patients' health,
  - for the patients themselves,
- the patient may give his or her required consent online easier than offline.

Health information in networks could also be used for research and quality management purposes. The wider implications of this development are not for this Working Group to be discussed. It should, however, be noted that electronic health information in a network generally might attract the interest of third parties such as insurance companies and law enforcement agencies.

The special sensitivity of health information has to be kept in mind when considering the online availability of electronic health records. Under the Hippocratic Oath[2] doctors have always had to treat patients' information confidentially. To care for the health and the life of the patient has never been a licence to disclose such information to third parties who are not participating in the treatment of the individual patient.

[1] Working Paper on Web-based Telemedicine, adopted on 27 March 2002 at the 31st meeting (Auckland), updated on 6-7 September 2005 at the 38th meeting (Berlin) <http://www.datenschutz-berlin.de/attachments/184/wpmed_en.pdf>

[2] "All that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal. If I keep this oath faithfully, may I enjoy my life and practice my art, respected by all men and in all times; but if I swerve from it or violate it, may the reverse be my lot."

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

Today the confidentiality of medical information is protected by criminal law in most countries. In some countries even the seizure of patients' health records for law enforcement purposes is forbidden as long as the records are in the possession of the doctor or a hospital. This standard has to be maintained once electronic health records are to be put online. The level of protection for the patient's health information cannot depend on whether it is stored conventionally in a file or on a network.

Health records are among the most sensitive and private information concerning an individual. Disclosure of a medical condition or diagnosis could negatively impact an individual's personal and professional life. Even the disclosure of a minor health issue could cause embarrassment to a patient, potentially making the individual weary to seek future professional medical advice. Examples of discrimination following the unauthorized release of medical data also exist in traditional paper filing systems[3]. Individuals have been denied employment, insurance, and mortgage approval due to the disclosure of medical information to unauthorized parties. Maintaining health records in an electronic form increases the risk that patients' information could be accidentally exposed or easily distributed to unauthorized parties.

Furthermore, the advent and use of the inherently insecure Internet and even more so of unprotected wireless networks[4] for storing and communicating health information causes particular concern.

Recommendations

Therefore the Working Group makes the following preliminary recommendations which will have to be reviewed in the light of future legal developments and technological innovations:

1. It must be carefully evaluated which categories of medical data should be made available in electronic form or put online. Certain categories of health information such as genetic or psychiatric data may have to be excluded from online processing altogether or at least be subject to especially strict access controls.

2. In any event it should be left to the patient's autonomous and freely taken decision, supported by means of user-friendly technology, what personal health information is to be stored and disclosed to whom in his or her e-health record or in a network unless expressly required by national law. This decision shall be without prejudice to the possibility for the relevant health care body or doctor to store this information for treatment purposes. Consent must always be a fundamental requirement in the medical scope. Strict purpose limitation is essential also in an online environment. To this end, a health care body needs to implement an internal access control system sufficient to protect the privacy of the patient.

[3] See generally, Health Privacy Project, Medical Privacy True Stories (Nov. 10, 2003), available at http://www.patientprivacyrights.org/site/DocServer/True_Stories.pdf?docID=321.

[4] See the Working Paper on potential privacy risks associated with wireless networks – Main Recommendations; adopted on 15 April 2004 at the 35th meeting in Buenos Aires <http://www.datenschutz-berlin.de/attachments/197/1_en.pdf>

3. The patients shall be fully informed on the nature of the data and the structure of the electronic health record containing them. Patients should have alternative (conventional) means to access medical data related to him or her.

4. There are additional confidentiality challenges inherent to the online availability of health records. Maintaining the legal standard of confidentiality within a traditional paper record environment may be insufficient to protect the privacy interests of a patient once electronic health records are put online. Personal health information may only be processed in open networks, if it is protected by strong encryption and secure authentication mechanisms. Only authorised, medically qualified personnel should be allowed to access specific parts of the e-health-files online where it is strictly necessary and an audit-trail should be available . The data have to be kept accurate and up-to-date. The patient should have a user-friendly means to access their personal audit trail online to be able to determine who has accessed his or her health record.

5. The Working Group recommends the development of baseline security standards for the handling of electronic health data. The baseline needs to include standards for data encryption, authorization mechanisms, transaction audit procedures, and access control systems. The development of baseline standards would enable information officers and custodians of records to ensure patient privacy protection and enjoy the benefits of an electronic records system. The Working Group encourages all the stakeholders (public authorities, health care sector, industry and standardisation organisations) to develop and apply privacy-compliant e-health technology which provides for the necessary confidentiality and security. The Working Group welcomes the initiatives at present under consideration at the International Organisation for Standardisation (ISO) to approve a security standard for the health and medical sector (with the proposed ISO Standard 27799 adapting the information security management ISO Standard 17799 to the health sector). It has however to be noted that these international standards cannot substitute national legislation on data protection.

The Working Group invites the medical profession and the public to comment on these recommendations.