

International Working Group
on Data Protection
in Telecommunications

Working Paper on Web-based Telemedicine

- adopted at the 31st meeting on 27-27 March 2002 in Auckland -
- updated at the 38th meeting on 6-7 September 2005 in Berlin -

Telemedicine is the practice of medicine at a distance. The phrase is broad enough to encompass Australia's Flying Doctor Service, remote video consultation after injuries on oil rigs and a medical advice programme on TV or radio. However, this paper is concerned with web-based health services and their data protection implications.

The American Medical Association has observed that "access to medical information via the Internet has the potential to speed the transformation of the patient physician relationship from that of physician authority ministering advice and treatment to that of shared decision making between patient and physician".¹ Others may not be so sanguine. However, the growth in health information sites,² on-line support and discussion groups³ and the electronic transfer of health data over the Internet suggests that the Web will become an integral part of the delivery of health care.

The delivery of health services over the Web currently arises in three main settings:

1. The Web as forum for discussion of health issues.

This comprises web-based discussion groups, bulletin boards and mailing lists. Postings can be anonymous and the discussions may or may not be moderated. Information posted on these forums tends to be anecdotal rather than authoritative and does not normally involve the payment of any fee or subscription or the creation of a clinical relationship between poster and browser. On a professional level, there are private discussion groups to which a fee is charged and entry is restricted to some subset of the browsing public, such as doctors.

2. Web-based provision of health services from doctor to patient (e-doctors)

There have been some attempts to replicate the traditional doctor-patient relationship in cyberspace. Patients, who may have identified themselves at some point for billing purposes, submit private queries to doctors describing their symptoms. The doctor, whose name and qualifications are available on the site, may respond via email or secure web transaction, setting out advice and a suggested course of treatment. While a doctor will be unable to "lay hands" on a patient, a visual examination might be possible through use of a webcam (although this is not yet usual). National law will typically require that prescriptions to dispense drugs carry a physician's signature and it may sometimes be unethical to prescribe drugs without personally examining the patient.⁴

3. *The web as repository of medical records*

Sometimes, as a component of (1) and (2) above, there is an electronic repository of personal health records to which the subjects and their authorised health professional have access.

This paper is concerned with the web-based provision of health services.

A selection of data protection issues in web-based telemedicine

Ethical obligations and legal duties of confidentiality

A well-established component of the normal relationship between physician and patient is confidentiality. Doctor-patient confidentiality imposes obligations on the doctor with regard to the personal information of the patient. If a licensed doctor is involved in the provision of health care then the same ethical constraints apply, regardless of whether the doctor's consulting rooms are real or virtual. However there are issues to consider with regard to the privacy of users of on-line health services.

Issues can arise from the use of any transaction data generated in the course of interactions between doctor and patient. Transaction data can under certain circumstances be associated with other web use sessions and with individually identifying data. Prescription data is, for instance, of interest to drug companies. Another concern is basic trust. Users need to be satisfied that a website is a trustworthy repository for their medical information.

If websites of this nature are to succeed, the Web must first be considered an acceptable avenue for the delivery of health services. Privacy is one of the primary consumer concerns with regard to e-commerce, and the sensitive nature of health information heightens these concerns. Some attempts have been made to promote good practice and thereby public trust. An example is the Health On-Line Code of Conduct which requires that websites 'honour or exceed the legal requirements of medical/health information privacy that apply in the country and state where the Web site and mirror sites are located'.⁵ Another is the AMA Guidelines for Medical and Health Information Sites on the Internet.⁶ Such initiatives are sometimes backed up by self-regulatory web privacy seal programmes with external accreditation and complaints processes.

Collection use and disclosure

Data collection during a telemedical consultation can take place indirectly and even 'invisibly', unlike in a physical consultation. Websites often post privacy policies that state what data will be collected,⁷ but these rarely cover the use of third party cookies placed by advertising companies. The secondary use of transactional data, especially if combined with other personal data, would be of significant concern.. It is unlikely that issues surrounding transactional data or cookies will be well addressed by conventional ethical rules. This may be compounded by a close partnership that may exist between medical practitioners and drug companies.

Ethical and privacy issues can also arise if transactional data is combined with identifiable patient information for the purposes of research.

Accuracy

There may be aspects of medical advice for which web-based applications will be inappropriate for the foreseeable future. For example, where diagnosis cannot safely be undertaken without more complete information than can be supplied by the subject (although

the “second opinion” function will be possible so long as an examining doctor has already accurately recorded symptoms and conditions).

Security

There are security issues in the storage of medical data so that it can be accessed by doctors and patients over the web. TCP/IP is an inherently insecure medium,⁸ and methods to remedy this insecurity require effort and expenditure by the website holding the data. While the storage of medical information on-line makes good use of the Web’s global ubiquity, it also raises the possibility that remote access may take place from insecure locations such as Internet cafes.

The confidentiality of medical information is valued very highly by consumers, and strong security against unauthorised access would be an essential method of avoiding a breach of confidentiality. It may also be a popular selling point of any telemedicine website.

Positive benefits

Unsurprisingly, this paper has concentrated on areas of concern. Before concluding, it is worth noting aspects of web-based telemedicine which may enhance privacy:

- individuals may be empowered to access information, both their own personal medical records and health care advice, at virtually any time and any place in the world;
- web-based telemedicine provides an impersonal means by which to obtain a “second opinion” - some individuals have felt inhibited and embarrassed to request a second opinion in the traditional manner through their own doctor;
- cyber-dispensing is a modern equivalent of “mail order” and can diminish individual embarrassment, particularly in small towns, when filling prescriptions for medications to treat sexually transmitted diseases etc.

Recommendations

The sensitivity of personal medical data means that there must be rigorous adherence to data protection and privacy laws by web-based telemedicine providers. Where such laws do not apply, the generally recognised principles of fair information practice should be followed and all collection, use and disclosure of data should be with the informed consent of the subject. In addition to the normal range of privacy and data protection considerations, the following recommendations are made.

1. Web-based telemedicine sites must make their information policies clear to users. Part of this will involve posting a clear and explicit privacy policy. Special attention should be paid to informing individuals about aspects of the practice of telemedicine which may depart from usual face-to-face medicine. Ideally, there should be verification of compliance with published privacy policies (for example through periodic audit or through a web seal programme).
2. Web-based telemedicine sites should not surreptitiously collect personal data from users by use of active elements or cookies. If applicable law allows the placing of active elements or cookies, they should only be activated with the consent of the subject and their use should not be mandatory for individuals seeking medical advice. Any telemedicine website placing active elements or cookies should highlight this in its privacy policy.

3. Transactional data revealing personal data about visitors to telemedicine sites should not be made available to third parties. In particular, medical data collected should not be used for commercial purposes.
4. Traditional ethical obligations upon doctors and health care professionals must not be diminished by reason of the provision of services over the Internet. Professional associations should consider updating their ethical guidelines to ensure that best practice is maintained in the new environment.
5. Web-based telemedicine sites should comply with applicable guidelines on consumer protection and professional standards so as to ensure that any personal data collected, obtained, used or disclosed are fairly processed. For example, the AMA provides valuable guidelines for website content, advertising and sponsorship and e-commerce, each of which ought to be considered.
6. Strong security measures should be taken to protect any stored medical data on a telemedicine site (as well as personal data in transit). Such measures should include encryption.
7. The associations representing doctors and similar professionals should adopt appropriate guidelines. Auditing procedures (e.g. web seals) should be in place to verify the implementation of these recommendations.

¹ American Medical Association, "Guidelines for Medical and Health Information Sites on the Internet <http://www.ama-assn.org/ama/pub/category/1905.html>

² See www.medscape.com [LINK], a portal directed at doctors and interested laypeople.

³ For a survey of medical Internet use see www.hon.ch/Survey/FebMar2001/survey.html [LINK].

⁴ Pharmacists can dispense medications so long as they receive a prescription (they do not need to see the subject). For an example of a web-based dispenser, see CyberChemist at www.chemist.co.nz/pm/index.cfm [LINK].

⁵ Available at www.hon.ch [LINK]. An article in the Journal of Medical Internet Research critiquing that code appears at: www.jmir.org/2000/I/37 [LINK].

⁶ See footnote 1.

⁷ For a study suggesting that there is an inconsistency between the privacy policies posted on health web sites and their actual practices, see ehealth.chcf.org/view.cfm?itemID=12497 [LINK].

⁸ For a brief explanation of the reasons behind this see www.itsecurity.com/tutor/tcpip.htm [LINK].