Introduction

One of the great challenges facing humankind as we enter the new millennium is to make high
quality health care available to all. Traditionally, part of the difficulty in achieving equitable access
to health care has been that the provider and the recipient must be physically present in the same
place. Recent advances in information and communication technologies have increased the number
of ways health care can be delivered.

Telemedicine, the area where medicine and information and telecommunications technology meet,
is probably the part of this revolution that could have the greatest impact on health care delivery.
The prefix ‘tele’ derives from the Greek ‘at a distance’, and therefore, more simply telemedicine is
medicine at a distance.

The demand for sophisticated IT in health care has spawned the growth of a commercial that sold
However, much of the technology that has been developed by private industry has technical
problems (Kleinke 1998), is resisted by physicians (Anderson 1998), and raises difficult issues
pertaining to security, privacy and confidentiality. These issues need to be addressed in order to
ensure that the health information infrastructure that is developed balances the concerns of the
individuals against the needs of health care providers, researchers, and public health organizations.

This paper will discuss the threats and challenges in protecting telemedicine information. There are
three concepts to be distinguished and related to security of telemedicine:

- Privacy: The right and desire of a person to control the disclosure of personal health
  information.
- Confidentiality: The controlled release of personal health information to a care provider or
  information custodian under an agreement that limits the extent and conditions under which
  that information may be used or released further.
- Security: A collection of policies, procedures, and safeguards that help maintain the
  integrity and availability of information systems and control access to their contents.

Privacy

Privacy protection in the fields of healthcare and nursing care requires the following in order to
maintain client's dignity (1) knowing their health condition accurately and deciding service policy
they can receive; (2) giving them the choice to be informed or not in case they are in serious
condition; (3) confining data when clients want them to; (4) removing unreliable information that
may lead to misinterpretation.
In other words, privacy protection is (1) based on confidentiality between clients and providers, and to retain authenticity when recording adequate information with responsibility; (2) it should be purposive with client’s consents when it is transferred; (3) integrity; (4) availability and accountability should be guaranteed.

Confidentiality

The principle of confidentiality has been at the heart of medical ethics since the time of Hippocrates and has been developed by various codes, including the International Code of Medical Ethics which states that a doctor must preserve “absolute confidentiality in all he knows about his patient” even after the patient’s death.

The General Medical Council, which oversees the registration of medical practitioners and supervises the practice of medicine in the UK, has issued guidance on the protection of medical information in its booklet Confidentiality which restates the Hippocrates principle that:

Patients have a right to expect that you will not disclose any personal information, which you learn during the course of your professional duties, unless they give permission. Without assurances about confidentiality patients may be reluctant to give doctors the information they need in order to provide good care. For these reasons, when you are responsible for confidential information you must make sure that the information is effectively protected against improper disclosure when it is disposed of, stored, transmitted or received (General Medical Council 1995).

Electronics patient records (EPRs) and electronic health records (EHRs) transmitted over national and international networks offer unprecedented opportunities for health care but pose difficult new challenges to confidentiality. An unauthorized user could attempt to gain access to a computer system connected to a network or illegally intercept a transmission and, although systems can be made more secure by restricting access to sites and encrypting information, it is necessary to set out principles that clearly demarcate the boundaries between who should have authorized access to patient data and who should not.

We normally think of the medical record as a tool at the point of care—the doctor’s office, clinic, or hospital. It supports primary care physicians, specialists, nurses, and administrators and has contributions from the many testing and treatment services. It is a memory aid, to help a team of providers manage a patient during an encounter, to provide continuity of care from encounter to encounter, and to serve as an institutional record of care.

Medical records also serve a variety of functions for organizations not involved directly in care. Records are sent to insurers to justify payment for medical services rendered, and to detect fraud. They are used for quality reviews, administrative reviews, and utilization studies to manage the business aspects of healthcare. They are also used for societal purposes, such as medical research, public health management, social service and welfare system management, law enforcement, screening and licensing for professions such as airline pilots, and determining life insurance eligibility.
Despite signing general consent forms as a requirement for obtaining health care in the U.S, the great majority of people (patients and physician alike), have only a vague understanding of where health care data flows, often with little control of its use (Rindfleisch 1997).

**Public Concern about Security**

Protecting privacy and confidentiality of individual health information is a critical issue. A Health Information Privacy Survey in 1993 found that 27% of the respondents believed that their medical information had been disclosed to others without their consent (Lou Harris and Associates 1993). The same study reported that 24% of health care providers surveyed reported violations of patients' privacy that had occurred within their own organization. Concern for privacy has grown. The 1996 privacy survey found that 18% of the public felt that the use of patient records for medical research without the patient's explicit permission was inappropriate.

Moreover, 75% of respondents felt that the use of prescription data to detect fraud was unacceptable (Lou Harris and Associates 1993).

The public's concern has been raised by disclosures of significant violations of confidential medical information. In Indianapolis, the medical records of patients of a psychiatrist, who treated sexual problems, were inexplicably posted on a web site accessible to the public. These records contained identifiable information such as names, addresses, and telephone numbers. They also contained intimate detail of patients' sexual problems (Laidman, Woods 1999).

One result of public concern is patient behaviour that shields them from intrusive uses of their health information (Goldman, Mulligan 1996). In order to protect their privacy, patients pay for their own care, visit multiple providers so that there is no central repository containing their medical records, and withhold or lie about sensitive matters (e.g. mental health services). The 1993 privacy survey revealed that 11% of the public had not filed an insurance claim and 7% had decided not to see a health care provider for fear that disclosure of their health information might hurt their job prospects or ability to obtain insurance coverage (Lou Harris and Associates 1993). In 1995 the Harris privacy poll reported that almost 60% of the public had at some time refused to provide information to a company or business in order to protect their privacy. This lack of reliable information may compromise diagnosis and treatment decisions but also undermines the value of data that enters an EPR.

In a public opinion survey, it was found that patients were very concerned that details of their illness could be available to relatives or strangers (Tachakra, Mullett et al. 1996). There was strong preference for not having the teleconsultations video-recorded as the problems of storage are enormous. One comment was: “how do I know that someone won’t scoop an armful of videos and laugh at a whole lot of patients?”
Threats to Confidentiality

The most important threats to patient information confidentiality are as follows (National Research Council 1997):

**Accidental disclosures.** Medical personnel make innocent mistakes and cause unintentional disclosures. A conversation may be overheard between care providers in the corridor or lift. A lab technician may notice test results for an acquaintance. Information may be left on a computer screen where it can be seen by a passer-by, or email or FAX messages may be misaddressed.

**Insider curiosity.** Medical personnel abuse their record access privileges out of curiosity or for their own purposes. Some do so out of concern for the well being of fellow employees or family members. Some want to know about celebrities being treated. Some may be concerned about the possibility of sexually transmitted diseases in a colleague they are dating.

**Insider subordination.** Medical personnel knowingly access information and release it to outsiders for spite, revenge, or profit. Embarrassing health information about prominent people finds its way into grocery store tabloids or the public press with relative ease. The London Sunday Times reported in November 1995 that the contents of anyone’s (electronic) medical record in Great Britain could be purchased on the street for £200.

**Uncontrolled secondary usage.** Those who have access rights to patient information for a purpose in support of primary care may exploit that access for other purposes not envisioned in patient consent forms.

**Unauthorised access.** Vindictive former employees, angry patients, network intruders, or others may steal information, damage systems, or disrupt operations. However an NRC study of security practices in health care institutions in 1997 found no examples of detected outside intruder break-ins.

Security Challenges

**Attitude.** It follows that an important measure of success in implementing a security policy is that all groups of staff are aware of, agree with and observe procedures aimed at preserving security of information. However, this is by no means easy to achieve since it requires significant change in behaviour of staff. Indeed, many health care professionals are still reluctant to use computers at all and to be asked, for instance, to remember a new password every month only hardens their attitude. Health care organisations have knowingly compromised information security through less than satisfactory access controls simply in order to encourage all staff to use the computer systems. Once such compromise has been adopted, it is subsequently very difficult to convince users of the need to strengthen access control.

Reluctance to change working practices in order to make information more secure is widespread amongst health care professionals. Despite their general acceptance of the principle of patient confidentiality, health care professionals tend not to accept responsibility for information security.

**Ignorance.** This reluctance is due in part to a poor understanding of the measures necessary to achieve security (many of which are very simple and easy to observe). Doctors are a particularly
difficult group to teach about information security since they often believe they know all about confidentiality (through the Hippocratic Oath) and those other aspects of security are not their problem. Unfortunately, whilst they know about the principle of confidentiality, doctors' knowledge of the potential threats to computer systems and how they can best be prevented may be poor. Information security, data protection and human rights should be a prominent part of medical informatics courses during undergraduate training and in postgraduate education.

Conflicting demands. It is not only in the medical curriculum that information security has been suppressed. The attitude that protection of patient information is less important than direct patient care pervades planning and provision of clinical services in general. Obtaining adequate funding for information security in an environment of limited resources, therefore, becomes a significant challenge. Indeed, the expense of installation and maintenance of additional security controls is often cited as a reason for failure to adopt them.

In addition to financial constraints, there are increasing demands for access to personal health care data for the purposes of monitoring, regulation, audit and research. Managed care organisations, insurance companies and health authorities contracting services are seeking access to patient records to substantiate claims or detect fraud. Surveillance, epidemiology and research programmes systematically gather the patient clinical data to monitor health care practices and understand distribution, spread and control of diseases. The police seek information from medical sources that may lead to the identification of criminals or to the prevention of crime. It is the ready availability of large quantities of clinical information on computer systems that has made such investigations possible and of appeal to regulators and the public. The laudable aims of greater efficiency, accountability, liability and knowledge achieved through such systematic data processing are, however, putting at risk the fundamental principle of patient confidentiality (Applebaum 2000). The balance between openness and confidentiality is the subject of much debate, which, while it remains unresolved, prevents application of a consistent approach to the protection of clinical information.

Inadequate systems. Given the availability of many good technical solutions to achieving secure systems, it is disappointing that few of the commercial health care computer systems currently on the market have more than the most basic security features. Either there is no commercial gain in incorporating more stringent controls, or the purchasers have been unwilling to pay for, or to implement, more secure systems.

Poorly designed security controls often impose constraints or impediments to access that are unacceptable to clinical staff. Even passwords are considered by many to be awkward and unnecessary, particularly when enforced expiry is imposed. Re-establishing network connections can take so long that busy clinical staff avoid logging off between transactions on network workstations. Security measures must be practical, acceptable to staff and cause minimal disruption to the processes of care. Few commercial systems at present achieve these ideals. However, once appropriate access control and auditing is installed, staff scepticism soon turns to acceptance as they come to realise their importance and benefit (Denley, Smith 1999).

Inconsistent policies. The extent, to which individual health care facilities apply security controls to their own computer systems, can vary markedly. Inconsistent policies and procedures can lead to frustration, confusion and potentially even harm to patients. This is exemplified by differences in organisation's policy towards transmission of patient information by facsimile. Whereas best practice is to send patient-identifiable information by facsimile machine only in emergencies and
according to agreed protocols, the convenience of such means of communication has led many organisations to allow their routine and uncontrolled use. An organisation attempting to apply more restricted use of facsimile transmissions is then faced with complaints from other organisations with more lenient policies whose staff are frustrated that they cannot send or receive patient information by that means.

Many similar inconsistencies in security policies are becoming evident the more that patient-identifiable information is being communicated across organisational boundaries. There is a growing need for commonality in security policies and negotiated agreements between agencies that are sharing patient information. Without a clear framework of responsibility and accountability, such agreements will be difficult to achieve.

Conclusions

Ultimately, security and privacy of telemedicine is a “people problem”. Technology can help to ensure that only health care personnel access information they have a right and need to know, and that information gets from one place to another accurately and securely. But technology can do very little to ensure the person receiving the information will handle it according to confidentiality standards. That depends on ethics and an effective supervisory and legal structure that provide sanctions against detected misuse.

Security measures in telemedicine must be chosen and integrated rationally. The measures must be balanced so they protect against a realistic assessment of risks and costs. System managers must choose a set of technological interventions that provide effective protection against perceived threats to system security but which overall impose acceptable costs. This choice is difficult at best and no acceptable standards of performance exist. These remain to be defined and require ongoing updates of threat models; evaluations of technologies; reconsideration of integration and operation strategies; and education of management, systems staff, and users.

References


