AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 69

Telemedicine and Crime

Russell G. Smith

Medical practitioners, like others in society, are beginning to realise the enormous potential benefits which modern communications technology has for interacting with colleagues and treating patients. In remote areas of the globe, such technology may truly be described as life-saving, as consultations may be carried out and treatment provided even where the practitioner and patient are incapable of being present together in the same surgery. As in other areas of human endeavour, however, new technologies not only provide benefits for the community; they may also create opportunities for crime. This paper outlines some of the potential areas of risk which face medical practitioners who make use of on-line services in terms of their criminal and professional liability, and their vulnerability to victimisation. Various strategies are reviewed which seek to prevent and to control such forms of illegality.

Adam Graycar
Director

Telemedicine includes a wide range of services carried out through the use of computers and telecommunications networks:

> *storage and dissemination of patients' records for diagnostic purposes; image compression for efficient storage and retrieval of image data; image processing for diagnostic purposes; digital transmission of 2-D and 3-D medical images; computerised control of medical equipment; real time transmission of video images for physician-physician and physician-patient consultations; direct transmission of medical data to hospitals from medical devices attached to patients at home; "data mining" of large databases of patient records for use in medical education, diagnostics, and cost/benefit analysis; and dynamic control of medical hardware by the use of Virtual Reality tools and the National Information Infrastructure (Northeast Parallel Architectures Centre 1996).*

Already, medical practitioners in Australia are starting to make use of such technology (Yellowlees & Kennedy 1997). Many make use of electronic mail for communicating with colleagues and commercial agencies such as through the Health Communication Network (http://www.hcn.net.au/). Others make use of the Internet for professional research by obtaining access to medical journals and publication lists. Some medical journals with Internet sites include the *Medical Journal of Australia* (http://www.library.usyd.edu.au/MJA/mja/), the *British Medical Journal* (http://www.bmj.com/bmj/archive/curr.htm) and the *Journal of the American Medical Association*

April 1997

ISSN 0817-8542
ISBN 0 642 24037 X

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 06 260 9200
Fax: 06 260 9201

For subscription information together with a complete list of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au
or send an email to:
aicpress@aic.gov.au

(http://www.ama-assn.org/public/journals/jama/jamahome.htm). The National Library of Medicine also maintains a comprehensive on-line facility, MedWeb, based at the Emory University Health Sciences Center Library (http://www.gen.emory.edu/medweb/medweb.nlm. html). Educational institutions such as the Centre of Medical Infomatics at Monash University Medical School in Melbourne make use of on-line services in teaching (http://www.monash.edu.au/infomatics). Still others are able to obtain access to information provided by government and professional bodies such as the Australian Medical Association (http:// www.ama.com.au/).

Finally, some practitioners are starting to employ on-line technologies in the diagnosis and treatment of patients as well as for the maintenance of medical records (Crowe 1993). In Australia, the main applications of telemedicine have been in psychiatry with most of the sixty to eighty video-conferencing sites being devoted to this use (Yellowlees & Kennedy 1997, p. 262). It is this adoption of "telemedicine" involving direct patient care which creates the most profound ethical, legal and professional dilemmas.

This paper outlines some of the potential areas of risk for medical practitioners who make use of on-line services both in terms of their criminal and professional liability. The question of victimisation will also be addressed as medical practitioners, like other users of on-line services, have much to lose at the hands of cybercriminals. Finally, brief mention will be made of some of the strategies which could be adopted to prevent and to control such illegal and unprofessional conduct.

The Size of the Potential Problem

At the outset, it is helpful to consider the size of the potential problem. Because telemedicine is a developing field, no systematic research has been conducted of the medico-legal risks involved in its use. Rather, we are left with a number of anecdotal accounts which may be relied upon to give an indication of the nature and extent of the problem. We are, however, able to estimate the use of on-line technologies world-wide and to make use of such estimates as an indication of the size of the potential problem.

Globally, the Internet is said to consist of some 15 000 computer networks linked to 20 million users in over 175 countries (Simicevic 1994, p. 47). Around 600 000 Australians are already connected to the Internet while a recent survey of 3258 Australian households conducted by the Australian Bureau of Statistics, estimated that 262 000 individuals use the Internet from home through the use of personal computers connected to telephone wires via modems (Australian Bureau of Statistics 1996, p. 22). The remaining Internet users operate from places of employment or government agencies including libraries.

In a survey of medical students conducted by the Department of Community Medicine at Monash University, 90 per cent of those surveyed had some exposure to computers while 84 per cent considered a working knowledge of computers to be important or very important for their future medical careers (Kidd, Connoley, Cesnik & McPhee 1993).

The use of telemedicine is expanding rapidly throughout Australia with substantial investments in new technology taking place (Yellowlees & Kennedy 1997). In the United States, at least US$646 million was invested in telemedicine initiatives during the years 1994-96 (United States, General Accounting Office 1997, p. 21).

With the expanding use of computer and telecommuni-cations technology by all members of the community, and particularly medical practitioners, it is important for them to be made aware of the potential risks which such technology carries in terms of civil, criminal and professional liability.

Areas of Risk

Interception of Communications and Breach of Confidentiality

Because digital information travels across computer networks which are connected by wires, there is the possibility that communications may be intercepted and either observed and copied, or altered in some way. Technology also enables the electromagnetic emanations from computer screens, keyboards, cables, printers and modems to be scanned externally at distances of up to a kilometre (Jones 1996).

In one case in England, information passing over a Bank's computer network was scanned electronically and even though the information was encrypted, the code was broken and the bank and various customers blackmailed by threatening to disclose information to the taxation authorities unless the sum of £350 000 was paid (Nicholson 1989).

Such conduct provides a significant threat where on-line services are used for medical therapeutic purposes such as for the transmission of confidential information about patients, reports from consultants to general practitioners, pathology test results and particularly for the variety of on-line telemedicine procedures which will become available in the near future. Perhaps the greatest area of concern arises where intimate images of patients being examined are transmitted electronically. If providing a chaperone for female patients during examinations conducted in a private

surgery is difficult enough to arrange, one can imagine the problems associated with guaranteeing privacy in respect of on-line examinations. Although data may pass along systems in encrypted form, this is by no means entirely secure and medical practitioners could well breach confidentiality by transmitting personal information across computer networks.

In Britain, the government's proposal to have a fully-networked health records system failed principally through concerns over confidentiality. On 26 November 1995, the *Sunday Times* revealed how confidential medical records of prominent people had been obtained illegally from National Health Service staff and doctors' surgeries for £150, thus confirming predictions regarding the insecurity of on-line medical data banks (Davies 1996, p. 63).

In the United States, a panel of the National Research Council has recently identified a number of security risks associated with electronic patient records and recommended greater use of access restriction devices (Leary 1997). An example of such risks which recently took place in Pinellas County, Florida, involved the leak of a confidential computer disk which contained the names of almost 4000 individuals suffering from AIDS (United States, General Accounting Office 1997, p. 63).

Medical practitioners may also be the victims of illegal interception. There have been many instances in Australia and overseas of practitioners' private telephone conversations having been intercepted and transcribed recordings used in medical disciplinary proceedings (*Edelsten v. Investigating Committee* (NSW) (1986) 7 NSWLR 222; *T v. Medical Board of South Australia* (1992) 58 SASR 382; and Smith 1994).

Intercepted communications which pass over the Internet are also likely to be used as evidence in proceedings before the criminal courts, civil courts in negligence and defamation actions and Medical Board proceedings. Intercepted information may also be used for commercial activities. In one case in the United States, for example, a bank manager paid a health official to check computerised health records of loan applicants, thus requiring the official to breach confidentiality (Anonymous 1996).

Hacking, On-line Vandalism and Terrorism

Hacking refers to the act of gaining unauthorised access to computer networks such as the Internet. Where unauthorised access takes place in order to inflict damage to the computer system or the information contained within the system it may be described as computer vandalism, and where this is carried out for extortion or political reasons, it may be termed on-line terrorism. Such activities may take a variety of forms.

The first entails the destruction of data files which may have serious consequences for medical research. In one reported case in 1989, for example, an AIDS research laboratory at the University of Bologna, Italy, lost ten years of irreplaceable data through computer vandalism (Clough & Mungo 1992, p. 141).

The second involves the encryption of data files to impede their accessibility. One recent case of this involved an individual who gained access to a hospital's computer system resulting in an operation being delayed for six days while essential data were located (Day 1996).

A third form of hacking involves gaining access to systems and altering data. Some examples of this which have recently taken place involve the substitution of pathology test results, the intentional alteration of drug doses in a paediatric ward of a hospital, and a nurse in one hospital who modified patient records relating to patients' prescriptions, scheduling of X-Rays, and recommended dates for discharge from hospital (Day 1996).

Finally, computer vandals may install viruses and other destructive and disruptive devices into hospital computer systems in order to demonstrate their ability to gain access to systems. The offenders may then seek to extort money from the hospitals concerned (*see* Cheong & Kidd 1997).

Because telecommunications systems are now being used to facilitate organised criminal activities such as conspiracies, money laundering, paedophile rings and drug trafficking (Schwartau 1995), the potential exists for terrorist organisations to extort funds from hospitals by threatening to destroy or alter computerised records, or in the case of telemedicine, on-line operations could be disrupted or medical records stolen unless funds are provided. Encryption technology is also being used by offenders to make their transactions secret and unable to be detected by law enforcement agencies (Shenon 1995).

Advertising and the Transfer of Funds Electronically

Medical practitioners are subject to a number of ethical and legal rules which restrict their commercial activities, particularly advertising of their services (*see* for example, section 64, *Medical Practice Act 1994* (Vic)).

Because the Internet, in particular, provides such a comprehensive and efficient medium for advertising, it is likely that it will be used to market health care products and services. When systems of electronic cash for use on the Internet are fully developed, Internet commerce will greatly increase. Already, however, it is possible to buy various products and services on the Internet by providing one's credit card number.

Many advertisements for commercial products and services are, however, deceptive, misleading or simply fraudulent. Various frauds involving health care products and services have been identified

including alleged cures for cancer (Varney 1996). These are much the same as other fraudulent health product scams but may be carried out much more extensively on the Internet with approaches being made to substantial numbers of individuals. There are even, so-called, "sucker lists" available on the Internet which identify previously defrauded individuals as being likely targets for future telemarketers (reference withheld).

Other aspects of the provision of health care also involve the use of tele-communications systems. Substantial sums of money are already transferred across the globe electronically by both wholesale and retail financial institutions. In Australia, the Health Insurance Commission makes substantial use of electronic accounting systems for the payment of health service providers and the reimbursement of users.

In the future, the Internet is likely to become one of the principal means of transferring funds electronically and already various electronic cash systems have been developed in the United States and Europe which enable funds to be stored and transferred via the Internet (Australian Payments System Council 1996). One can imagine the situation developing in which telemedicine procedures will be paid for using electronic cash, and, indeed, all health care consultations may be paid for electronically.

Such systems are likely to be targets for fraud and illegality in the same way as other electronic funds transfer systems have been used to steal funds. The American Bankers' Association recently estimated that US$5 million per annum was lost through on-line fraud in the United States alone (Holland 1995, p. 88).

Because both health service providers and users make extensive use of electronic funds transfer systems for billing and payment of health services, they have much to lose at the hands of fraudsters. In an already constrained health service industry, substantial losses through fraud simply could not be sustained without resulting in severe disruption to the provision of services.

Copyright Infringement

Medical practitioners who are involved in research and publication may be at risk of breaching copyright when using on-line services such as by downloading material from the Internet without appropriate authorisation. Similarly, they may, themselves, be the victims of on-line piracy and other forms of intellectual property crime.

Placing works on the Internet by no means ensures that an author's intellectual property rights will be respected and there have been many reported instances of substantial infringements taking place on the Internet, principally through illegal copying of computer software (Meyer & Underwood 1994, pp. 68-9).

In the future when many forms of medical practice may become dependent upon on-line access to information, the risks associated with unauthorised electronic copying of data will be enhanced. Although infringement may not immediately result in professional liability in terms of medical disciplinary proceedings, where copyright infringement is accompanied by breach of confidentiality or other forms of unauthorised disclosure, medical licensing authorities may take an interest, particularly where criminal liability has also been established.

Unprofessional Conduct on the Internet

If one examines the various Codes of Professional Conduct which are published by the State and Territory Medical Boards, and the Australian Medical Association's Code of Conduct, it is apparent that medical practitioners who make use of on-line services could infringe many of these ethical rules.

Any on-line conduct which results in a criminal conviction clearly falls within the jurisdiction of registration authorities. Conducting professional examinations or prescribing drugs through the use of communications technologies without having conducted a proper examination of the patient has previously resulted in findings of guilt of professional misconduct (Smith 1994) and the use of telemedicine will create further risks of this nature. Failure to respond to a patient's requests for assistance made by electronic mail, for example, could also be unprofessional if the practitioner has inadequate systems in place to record and to monitor in-coming calls. Breach of confidentiality and the improper use and maintenance of medical records kept on-line are considerable areas of concern as already discussed, while im-proper delegation of professional duties to inadequately trained colleagues may occur where practitioners are not directly involved in providing on-line treatment themselves. Where practitioners use on-line services for advertising in breach of legal or ethical requirements, they may be dealt with in disciplinary proceedings. Finally, there is the potential for engaging in unregistered practice where a practitioner uses telemedicine to treat patients in a jurisdiction which does not recognise his or her registration.

Many of these potential areas of risk raise similar issues to conduct carried out using less sophisticated technology. Already the Medical Practitioners Board of Victoria has guidelines on the use of telephones in the treatment of patients, and similar rules will need to be created with respect to telemedicine. The British Medical Association's *Code of Conduct*, for example, has had a section which specifically refers to the problems of confidentiality in telemedicine since 1993 (British Medical Association 1993, pp. 38-9).

Preventive and Control Strategies

Various strategies may be used to prevent and to control these forms of illegality and unprofessional conduct, some of which entail the use of traditional enforcement techniques while others rely on technology itself. Of primary importance, however, is the need for practitioners to be made aware of the risks associated with using on-line medicine. Many of the vulnerabilities are already common knowledge in the computer and communications world and the Internet, itself, provides many sites which alert users to potential risks. Medical associations and registration authorities should, however, also play a role in developing guidelines for practitioners and alerting them to the risks in terms of civil, criminal and professional liability.

Technology may also have a role to play in preventing undesirable on-line conduct from taking place. The use of encryption is the primary method by which confidential information is safeguarded in on-line communications with the power of the encryption algorithm used being directly proportional to the need to safeguard information. For example, much stronger encryption may be required for the transmission of an HIV test result than for a patient's request for a consultation. Biometric access control mechanisms may also be used to ensure that only specified individuals are able to gain access to computer networks. Patients about to embark upon a telemedicine consultation may, for example, be required to undergo thumbprint or retinal scanning.

Telecommunications carriers and service providers are also able to take a number of steps to ensure that networks are not used for improper purposes, and, indeed, in the United States service providers may be held liable in civil proceedings for failing to take steps to detect and prevent illegal conduct which comes to their attention (Cook 1991).

Finally, various reforms can be introduced to ensure that traditional enforcement strategies operate efficiently and effectively to control on-line illegality and unprofessional conduct. Just as law enforcement agencies have specialist units for the investigation of computer crime, so medical registration authorities will need to engage investigators trained in the technologies of telemedicine. Most likely, consultants will be used in the first instance to assist Boards in preparing guidelines and in investigating complaints in this area.

Guidelines setting out proper professional practice for on-line medicine also need to be created which, ideally, should be uniform across jurisdictions. One of the central problems with law enforcement in relation to on-line activities is that conduct invariably involves a number of individuals in a number of jurisdictions. Close cooperation between agencies is required and uniform rules and procedures are essential.

Conclusion

Telemedicine and other computer-based technologies which are used by medical practitioners could be seen as a double-edged sword: on the one hand, they may greatly facilitate the provision of treatment to people, particularly in remote locations or in emergencies; while on the other hand, they may provide enormous opportunities for the commission of illegal and unprofessional conduct. The loss and damage which could result from the improper use of on-line technologies are formidable, both in financial and human terms.

Agencies charged with the regulation of medical practice need to take prompt action to ensure that practitioners are made aware of the risks associated with conducting medicine in cyberspace and that professional rules of conduct clearly delineate proper from improper uses of communications technologies. Close cooperation is needed between all those involved in providing on-line medical services to ensure that they are used in a manner which protects both users and providers from some of the more undesirable possibilities which new technology facilitates.

References

Anonymous 1996, "Medical records face hacker risk", *Security Australia*, vol. 16, no. 10, p.18.

Australian Bureau of Statistics 1996, *Household Use of Information Technology*, Australian Bureau of Statistics, Canberra.

Australian Payments System Council 1996, *Annual Report 1995-96*, Reserve Bank of Australia, Sydney.

British Medical Association 1993, *Medical Ethics Today: Its Practice and Philosophy*, British Medical Association, London.

Cheong, I. R. & Kidd, M. R. 1997, "Safe practices in cyberspace: A medical perspective on computer viruses", *Medical Journal of Australia*, vol. 166, pp. 44-6.

Clough, B. & Mungo, P. 1992, *Approaching Zero: Data Crime and the Computer Underworld*, Faber and Faber, London.

Cook, W. J. 1991, "Paying the bill for hostile technology: PBX fraud in 1991", *Computer Law and Security Report*, vol. 7, no. 4, pp. 174-7.

Crowe, B. L. 1993, *Telemedicine in Australia*, Australian Institute of Health and Welfare, Canberra.

Davies, S. 1996, *Monitor: Extinguishing Privacy on the Information Superhighway*, Pan Macmillan, Sydney.

Day, K. 1996, "Defending yourself and your organisation from infor-mation warfare", paper presented to the Information Warfare and Competitive Intelligence Conference, 27-28 November, Sydney.

Holland, K. 1995, "Bank fraud: The old fashioned way", *Business Week*, 4 September, p. 88.

Jones, F. 1996, "Nowhere to run . . . nowhere to hide: The vulnerability of CRT's, CPU's and peripherals to TEMPEST monitoring in the real world", http://www.thecodex.com/c_tempest.html

Kidd, M. R., Connoley, G. L., Cesnik, B. & McPhee, W. 1993, "What do medical students know about computers?", *Medical Journal of Australia*, vol. 158, pp. 283-4.

Leary, W. E. 1997, "Panel cites poor security on medical records", *New York Times Fax*, 6 March.

Meyer, M. & Underwood, A. 1994, "Crimes of the Net", *Bulletin/ Newsweek*, November pp. 68-9.

Nicholson, E. 1989, "Hacking away at liberty", *Times (London)*, 18 April.

Northeast Parallel Architectures Center (NPAC), Syracuse University, Syracuse, New York 1996, "Telemedicine", http://www.npac.syr.edu/users/ensmingr/TMED.html

Schwartau, W. 1995, *Information Warfare: Chaos on the Electronic Superhighway*, American Society for Industrial Security, Arlington.

Shenon, P. 1995, "World Trade Centre suspect linked to plan to blow up two planes", *New York Times*, 26 March, p. 37.

Simicevic, D. 1994, "A bold move by UWS opens up Internet system", *Sydney Morning Herald*, 11 April, p. 47.

Smith, R. G. 1994, *Medical Discipline: The Professional Conduct Jurisdiction of the General Medical Council, 1858-1990*, Clarendon Press, Oxford.

United States, General Accounting Office 1997, *Telemedicine: Federal Strategy is Needed to Guide Investments*, Report to Congressional Requesters No. GAO/NSIAD/HEHS-97-67, General Accounting Office, Washington.

Varney, C. 1996, "Regulating cyberspace: An off the record interview with Federal Trade Commissioner Christine Varney", *Computer Underground Digest*, 25 March, no. 8(24).

Yellowlees, P. M. & Kennedy, C. 1997, "Telemedicine: Here to stay", *Medical Journal of Australia*, vol. 166, pp. 262-5.

Dr Russell G. Smith is a Research Analyst with the Australian Institute of Criminology

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia