SAMJ
ARTICLES

The protection of personal and medical data — a call for confidentiality

C. Els, T. Verschoor, H. Oosthuizen

Personal data and privacy are increasingly being threatened by a boom in technological development — the replacement of conventional networks of communication with the perfected combination of computer and telecommunications. The subsequent high degree of transparency has the potential to damage the individual's right to 'informational self-determination'. The most common ways of unlawfully entering a computer data system, the reasons why an individual's information is treated as confidential and the ethical issues involved, international and local statutory instruments that protect such personal information, and ways to stop the outflow of personal information are discussed.

S Afr Med J 1995; **85:** 773-775.

> 'The computer with its insatiable appetite for information, its image of infallibility, its inability to forget anything that has been put into it, may become the heart of a surveillance system that will turn our society into a transparent world in which our home, our finances, our associations, our mental and physical condition are laid bare to the most casual observer.'[1]

On the verge of the year 2000 we are enjoying the convenience of a society in which communication plays a vital role. The revolution has finally arrived — the replacement of conventional networks of communication with the perfected combination of computer and telecommunications. The inevitable consequence is the creation of a bank of personal, medical and social data, with a degree of transparency never seen before. For more than 25 centuries, a tradition of sensitivity to confidentiality has been maintained in the context of the doctor-patient relationship. This privacy, acknowledged virtually world-wide, is increasingly being threatened by the technological boom and the ongoing development of ever more sophisticated communication networks. Even the 'causal observer' will be able to gain access to information, thus potentially infringing the individual's right of 'informational self-determination' with a consequent breach of confidentiality.

Departments of Psychiatry and Criminal and Medical Law, University of the Orange Free State, Bloemfontein

C. Els, M.B. CH.B.

T. Verschoor, B.IURIS, L.L.B, L.L.D.

H. Oosthuizen, B.IURIS, L.L.B, L.L.D.

The computer and data

The Oxford Dictionary defines 'computer' as an 'electronic apparatus for analysing or storing data, making calculations or controlling machinery'. The computer is a compact electronic instrument, working on the principle of binary codes; it distinguishes only between 0 and 1 and thereby memorises and retains data. This article will focus on 'personal data', which comprise data relating to an identified or identifiable natural person (Convention 108, 27 May 1982).[2]

Old clinical records are being replaced by electronic memories, ready and available at less than a moment's notice provided a request is suitably programmed.

Large quantities of patient information are stored in a small space. This information is easily retrieved and analysed. Communication of patient information has become an easy and convenient part of the overall management of a patient, for example between the treating physician and the pathology laboratory or the medical aid scheme. But in the storage of data lies the problem of confidentiality, because the communication thereof has legal implications. Privacy and the protection thereof are important legal issues.[3]

The electronic data dilemma

In psychiatric practice (private and hospital), the handling of stored data is carefully restricted by the treating physician. Access to confidential information is prevented by reasonable steps taken by the physician. Van der Poel and Smit[4] state: 'It would have taken a very determined, devious and enterprising person to gain unauthorized access to such confidential information — an occurrence that, under normal circumstances, the law cannot require a practitioner to foresee.' But how safe is the computerised system of data storage?

'I don't need jackhammers and atom bombs to get in when I can walk in through the door', says Silliam Cheswick, a network security specialist at AT+T Bell Laboratories in the USA. In the professional (computer) scenario, security has been described as 'so lax that passwords and other protective devices are almost a waste of time'. Most common ways of (unlawfully) entering a computer data system include the following.[5]

Password sniffers

These are small computer programmes deliberately entered into a computer network. The explicit aim of such a 'sniffer' programme is to identify and store any key- or password for retrieval by the writer of the programme.

Spoofing

To exploit security holes from the inside of the computer system, it is first necessary to gain access to the programme itself. Step two is the installing of a sniffer programme like a 'little back door' or a secret return path back into the programme.

The hole in the web

It is possible for an unauthorised person to enter a computer data network (web) without clearance or a secret password. Because of the ease with which computerised data can be accessed, protective measures should be introduced.

Medical secrecy

There are four reasons for treating personal information as confidential.[4]

Medical ethics

'All that may come to my knowledge in the exercise of my profession or outside of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal.'

The oath of Hippocrates underlines a basic element of the doctor-patient relationship. This ancient declaration of the individual's right to privacy is acknowledged world-wide and has been supplemented by statutory instruments, international conventions and declarations.[6,7]

Problems do, however, arise with the electronic processing of medical data. Confidentiality and secrecy alone do not protect the patient's right to informational self-determination. Often many people are involved in this processing, many of whom are non-physicians. Callens[2] details further problems in the processing of personal medical data, e.g. that data can be collected and stored in a relatively short period of time, and that the individual is not protected by the liability resulting from a physician's negligence in disclosing confidential information. He stresses that extreme prudence is necessary to protect the individual.[2]

Statutory instruments

Rule 16 of the ethical code for medical practitioners promulgated in terms of the Medical, Dental and Supplementary Health Services Professions Act 56 of 1974, deals with professional secrecy and reads as follows:

> 'Divulging verbally or in writing any information which ought not to be divulged regarding the ailments of a patient except with the express consent of the patient or, in the case of a minor, with the consent of his parent or guardian, or in the case of a deceased patient, with the consent of his next-of-kin or the executor of his estate.'

This rule specifies acts or omissions in respect of which the council may take disciplinary steps.

South African common law

One's personal rights (e.g. to a good name, dignity and privacy) are protected by a variety of legal rules. Violation of any of these rights constitutes possible defamation, contempt or invasion of privacy.[4]

The intrinsic value of information (as a means of earning a living)

Knowledge is power. It has monetary value and is protected by the law. The unlawful disclosure of information may be potentially damaging or hazardous — the dignity of a person may be affected, rendering the disclosing physician liable.

> 'It is clear that where use is made of a computer in the storing or processing of patient data, there is a special risk of both an ethical and a legal sequel where other parties may also have access to the information stored in the computer. It goes without saying that intimate medical data which gets (*sic*) into the hands of the wrong people can cause great harm to a person's career and personal relationships.'[8]

International and local legal tools

'Any blow to human rights is a perversion leading to the decay of law.'[7]

Most countries in the Western hemisphere have statutes restricting the processing of data. In South Africa no legislation aimed at the explicit and sound protection of the individual's right to privacy and identity exists. Neethling[1] recommends the introduction of adequate legislation in this regard. It could be restricted to the data processors currently posing a potential threat to the individual's privacy: the government, credit bureaus and insurance companies.

The current interim constitution of South Africa guarantees freedom of speech and expression, [9] but there is also a provision that guarantees freedom of information.[9] What does this imply? If the government possesses information, you have the right to gain access to it (excluding of course information on matters of national security, commercial confidentiality, law enforcement and issues concerning personal privacy).

A fine line needs to be drawn between public and private interest. In weighing the public interest against that of the individual, Dierks[6] describes four areas covering nearly all possibilities of medical data flow, namely: (*i*) the aim of processing data is therapy — the individual's interest is in his/her desire for health; the public interest entails the health of the people; (*ii*) health and insurance systems; (*iii*) administrative areas; (*iv*) research, where the individual's interest is not self-evident.

German legislation has laid down five criteria/guidelines for the protection of data:[6] (*i*) the right to informational self-determination is a constitutional right (embracing all personal data); (*ii*) personal data may only be transmitted or processed to serve a distinct purpose that is in the public interest; (*iii*) the process itself must be covered by a formal statute in accordance with the constitution; (*iv*) all interested parties affected must be reconciled; and (*v*) reasonable safety procedures are required for the process.

South African criminal law does not provide sufficiently for the protection of personal data. Malan[3] is of the opinion that protection is lacking in three respects: (*i*) it does not criminalise unauthorised access to a computer; (*ii*) it makes no provision for the unauthorised alteration or forgery of data; and (*iii*) the unauthorised obtaining of a trade secret is not penalised.

In the international arena, however, article 17 of the International Covenant on Civil and Political Rights of December 1966 reads:

'Member states must forbid the computerized processing of health related data without the relevant person's free, explicit and written consent.'

Disclosure of data on personal matters, racial or ethnic origins, sexual life, political, philosophical or religious opinions and mutual insurance relationships is prohibited.[7]

What protective measures should be introduced?

1. Ethical codes of conduct for every operator/person involved in the processing of data.

2. Maximum control of his own personal data by the individual. The individual must: (*i*) be aware of the mere existence of a databank containing his personal details; (*ii*) be aware of the aims of processing the specific data; (*iii*) have access to the data; (*iv*) have access to the names of all people who have had access to his personal data; and (*v*) be able to negotiate the alteration or deletion of specific data.[1]

Conclusion

South Africa falls far behind international measures to protect personal medical data. Currently, there is no specific legislation to protect the individual's right to informational self-determination. Processing clerks at hospitals and non-treating physicians have free access to personal medical data. No codes of conduct exist for the management and control of computerised medical data. Private physicians and their receptionists electronically communicate private medical data to medical aid schemes, laboratories and the like, with no guarantee that such data will not be divulged to unauthorised third parties.

It is suggested that legislation for the protection of personal data be given higher priority. In the interim, physicians, hospitals and supplementary health services are encouraged to take all reasonable steps to prevent unauthorised disclosure and access to the individual's personal data.

REFERENCES

1. Neethling, J. *Persoonlikheidsreg*. 3rd ed. Durban: Butterworths, 1991.
2. Callens SH. The automatic processing of medical data in Belgium — is the individual protected? *Med Law* 1993; **12:** 55-59.
3. Malan FR. Oor inligting, rekenaarmisbruik en die strafreg. *De Jure* 1989; **22**(2): 211-232.
4. Van der Poel KG, Smit PC, Protection of computerized medical data — a problem? *S Afr Med J* 1985; **68:** 106-109.
5. Quittner J. Cracks in the net. *Time* 1995; 27 Feb: 36-39.
6. Dierks C. Medical confidentiality and data protection as influenced by modern technology. *Med Law* 1993; **12:** 547-551.
7. Thiry E. Personal medical and social data: their processing and legal protection. *Med Law* 1993; **12:** 643-649.
8. Strauss SA. Professional secrecy and computerisation of patient data. *South African Practice Management* 1985; **6:** 5.
9. *Constitution of the Republic of South Africa*. No. 200 of 1993; Pretoria. Government Printer, 1993.

Accepted 11 Apr 1995.