on the Read codes, which are already used in primary care and other areas of the NHS. Access to any of this information will be possible, however, only if computer systems throughout the NHS are compatible. The timetable is short. The central component of the network is planned for next year, and the whole strategy could be complete by 2000.

The project is huge, ambitious, and driven largely by the internal market's need for high quality information for contracting; at the moment it is going ahead with little input from the health professionals whose duty it is to protect sensitive patient information. Last week's seminar heard that patient privacy is threatened by both the scale of the project—more information, and more people with access to it—and its universal nature. A large database with up to date details, including names and addresses of everyone in Britain, would be a tempting target for many commercial and governmental organisations. It also heard that current laws are inadequate to protect patient confidentiality in this sort of system.

Many concerns relate to computerisation in general: the theft of computers, hacking, computer viruses, inadvertently sending patient details to the wrong person, and the depersonalised nature of information on a computer screen. Anthony Nowlan, a clinical research fellow at Manchester University's department of computer science, told the seminar that without the personal quality of paper notes it was easier to breach confidentiality by, for example, forgetting to log off a ward terminal or leaving passwords taped to the front of it. Finally, of course, computers allow searches to be conducted among vast amounts of data in ways that would simply be impracticable with paper records.

As important are issues of ownership, control, and use of any national network and how effective current data protection laws would be in preventing abuse of the information on the network. Simon Davie, director general of Privacy International, an independent organisation of experts committed to protecting personal privacy, warned the seminar of the dangers of relying on the integrity of governments to prevent abuse of such a uniquely comprehensive, up to date, and reliable population register. It is not only possible, he said, but probable that without specific safeguards the system would end up linked with other services such as social services, education, and law enforcement, none of which are governed by workable ethical codes. A health register could also be used as the basis for a national identity system, with all its attendant risks of invasion of civil liberty and national surveillance.

The use of electronic information about people is governed by the Data Protection Act 1984. The eight principles of the act set conditions for registered users such as NHS trusts, family health services associations, and general practitioners. One states that personal data can be used only for the purposes it was registered for and given only to the people described in the register entry. There are, however, few restrictions on who can be named. For example, it would be theoretically possible for a trust hospital to alter its register entry to allow it to divulge health information to a health insurance company. Trusts obviously have a duty of confidentiality to patients but that duty is not governed by statute. The data protection registrar, who administers the act, said in his 1993 report to parliament, "I have doubts whether common law, non-statutory guidance, or professional codes will be sufficient (to prevent compromising the confidentiality of sensitive health information). The common law duty of confidence is complex and does not appear to have been tested in circumstances such as the wide use of health information in the NHS."[3]

In 1990 the BMA published, on behalf of an interprofessional working group chaired by Sir Douglas Black, a code of confidentiality governing the use and disclosure of personal health information.[4] It emphasises that patient information must be held only for the purposes of health care and disclosed only to those who need to know it. The data protection registrar has been urging the government since 1991 to adopt this code, which would go a long way to protect patient privacy. Instead the Department of Health promised its own guidelines. These have yet to be published.

It is clear that there is a tension between sharing information, with all its benefits for patients and for health professionals, and the fundamental human right of personal privacy. What the balance between the two should be is debatable, but doctors and their patients need to be well informed about the strategy and its implications so they can shape the debate. Meanwhile, the British Medical Association will be campaigning for public awareness and for a code of confidentiality that is legally binding, effectively policed, and the ultimate responsibility of the secretary of state for health.

ALISON TONKS

Assistant editor, *BMJ*

1 Information Management Group, NHS Management Executive. *An information management and technology strategy for the NHS in England.* London: Department of Health, 1992.
2 Social Surveys (Gallup Poll) Ltd. *Computerisation in GP practices: 1993 survey.* Leeds: NHS Management Executive, 1993.
3 Data Protection Registrar. *Ninth report.* London: HMSO, 1993.
4 Inter-Professional Working Group. *Confidentiality of personal health information.* London: BMA, 1990.

Correction

The Gardner hypothesis

Owing to an editorial error Hazel Inskip's address was omitted from her editorial in last week's *BMJ* (6 November, p 1155). Dr Inskip works at the MRC Environmental Epidemiology Unit, Southampton General Hospital, Southampton SO9 4XY.