In 1994, Privacy Commissioner Bruce Slane advised a Wellington Medical School audience: “Privacy is not simply an absence of information about us in the minds of others, it is the control we have of information about ourselves”.

Mr Slane repeated this observation to the NZ Law Society in 1996.

The issue of “control” of personal information has arisen in the commentaries of several privacy experts on a number of occasions. Indeed, control is often seen as central to any consideration of information privacy. It is certainly not a new concept on the New Zealand scene.

Despite the widely held recognition of the importance of privacy, hard copy and computerised information systems seldom provide individuals with true control of their own personal information. The architects of such systems usually compromise personal information privacy in favour of utility of the systems they are designing.

In this regard, personal health records are worthy of special examination because of their sensitivity. Most individuals regard their health particulars as a source of potential embarrassment, even when those details are actually of no interest to anyone else. Additionally, health records may be subject to inappropriate snooping for various reasons, such as curiosity, jealousy, or personal gain.

Health consultations generally occur on the understanding that the information divulged by the patient to the practitioner will not be disclosed to others. Many health interventions would not occur at all if this implied contract between provider and user did not exist, particularly in sensitive areas such as mental health, sexual health, and drug & alcohol problems.

As is the case with many other record systems, personal health records are not truly private. It is more correct to state that they are available to a limited potential viewing audience, some of whom arguably should not have access to those records. For example, written files are available to anyone with physical access to them, including professional and clerical staff of the establishment, cleaners, and any member of the public who is left unattended in proximity to a hard copy of the information. Computerised records may be perused by anyone with a login to the system, or anyone with access to an unattended terminal. Personal records may be passed from one health provider to another with a minimum of formality. In this sense, patients do not maintain control of their own private information.

Patients do not usually recognise that sensitive information held by their personal health provider may fall into the hands of other, unintended, recipients; nor do most patients realise the frequency with which this transfer of personal information occurs.

Historically, this deficiency has been overlooked for two main reasons:
Firstly, personal health records were originally paper-based, often consisting of half a line of appalling scrawl on a tatty card that was locked away in some obscure office. Over the last twenty years, personal medical records have been stored with increasing frequency on small, isolated computer systems, and it is really only the last decade or so that larger networks have been used for this purpose. Even then, there has been a limited amount of interconnectivity between systems. Overall, it can reasonably be claimed that the opportunity for inappropriate disclosure of personal information has been relatively limited, until now.

Secondly, the triumph of utility over privacy has been tolerated because only a small number of relatively unsophisticated control systems have been available on the myriad of small, independent systems, and the implementation of the available control methods has been seen as an unnecessary expense and an impediment to the use of these systems.

However, the organization of health information systems is now changing.

In New Zealand, the Ministry of Health’s information strategy is concerned primarily with achieving the goals set out in the 2001 WAVE report. The WAVE document states, in part, that the health sector’s primary goal must be the integration of health information systems over a time frame of three to five years. Regarding the personal Electronic Health Record (EHR): “Ideally, the information should be available immediately at the point of care, irrespective of the patient’s location”.

Several important issues arise from these goals, three of which will be briefly explored here. These are:

- the notion that the wholesale distribution of personal health information is necessarily a good thing;
- the problems arising from the moral and legal responsibility to obtain informed consent to the sharing of information; and
- the risk of abuse of a distributed system, either on an individual level or an organisational level.

There appears to be widespread acceptance that personal health records should be available anywhere, at any time. At first sight, the idea seems to be meritorious. However, there is almost no academic evidence to either support or oppose the pursuit of this goal. Given that the health sector prides itself on its scientific, evidence-based decision-making processes, it is surprising that the notion of the ubiquitous electronic health record has such widespread favour.

There are certain instances where patient histories are very valuable. For example, an unconscious patient requiring surgery may be allergic to an anaesthetic drug. This specific piece of information is highly important, and perhaps it indicates a need for the MedicAlert database to be available on-line to hospitals. However, this type of case is not an indication that all the personal health details of this hypothetical unconscious patient should be available over a nationwide network. (As an aside, even a fully computerised information system would fail to be helpful if this patient could not be reliably identified). Fortunately, the primary management of most emergencies is not severely impaired by the absence of detailed medical records.
More commonly, the availability of a patient history is a convenient addition to the management of more routine cases, and can reduce costs due, for example, to the avoidance of unnecessary repetition of tests. However, these other factors are not, in themselves, sufficient to justify the nationwide connection of personal health records.

The second issue is the requirement to offer health consumers a choice whether all or some of their personal information will be available on a nationwide network. Currently, institutions such as public hospitals essentially only offer patients the option of providing or withholding information from the attending health provider. Once personal information is provided, the patient has virtually no control over the way that information is stored or distributed within the existing system. Beyond the boundaries of the institution, computerised patient records can be made available to other institutions and providers at the discretion of the management. Every institution has its own set of global policies regarding sharing of personal information, and each institution has its own set of safeguards to allegedly “ensure” that users will comply with those policies. Existing indications do not suggest that such distribution of patient records over a nationwide system will be subject to patient consent.

An essential part of the consent to store information on a nationwide network is the need to assure the public that individuals or groups cannot misuse personal health records, which raises the final point for fleeting consideration.

A major feature of computer technology is the ease with which information can be stored, transferred, processed, and matched. This capacity has led to fears about the ability of the technically literate, or even the State itself, to use information in ways that were not originally intended.

Previously, health records were only accessible to a limited number of individuals, each of whom had some direct relationship with the site of data storage. The systems did not provide full control to the individuals about whom information was stored, but this imperfection was tolerated for pragmatic reasons and because of the limited opportunity for dissemination of private information. In the case of a nationally distributed information system, by comparison, the problems and risks of abuse are increased exponentially. Potentially anyone with rights to log on to the system could gain access to anyone else’s personal files, irrespective of whether that access was justified.

On the individual level, such a degree of exposure is unsatisfactory. Of greater concern is the potential for systematic abuse of the system. As Tim McBride stated in 1994: “In the past, the creation of a massive State database was a recurring fear, as was seen during the controversy surrounding the establishment of the Wanganui Computer Centre in the mid-1970s. These days, the establishment of a big State databank is not the concern. Rather, it is the proliferation of databanks that can easily be linked together for information matching purposes”. A national electronic health record system involves the type of linkage of databases to which Tim McBride referred.

It is not appropriate for this paper to wander into a lengthy examination of the technical aspects of design and implementation of information systems. The coverage here will be restricted to four issues that the writer considers to be crucial to the ethical success of a widely interconnected health information system in general, and the ubiquitous electronic health record in particular.
**Issue 1: Time**

It is generally accepted that security and privacy provisions should be built into a computerized information system from the design phase, not applied later as patches.

It will not be easy to establish an acceptable formula for the delivery of robust personal privacy on a distributed health network. Much investigation, thought, consultation, innovation, and some degree of flexibility and compromise, will be required.

Many disparate systems already exist amongst health service providers. If the existing systems are interconnected in the near future, the task of providing uniformly robust personal privacy across the resulting internetwork will be fraught with difficulty. However, as weeks turn into months and years, other systems are being designed, implemented, and commissioned, adding progressively to the complexity of the problem. It will be far easier to introduce and safely integrate these new systems when a common standard has been established.

The process of developing an acceptable privacy standard will be lengthy. The process of development is best started now, because the scale of difficulty will only increase with time. If the task is delayed too long, it will become impossible to achieve in the available time. In this eventuality, privacy considerations will be sacrificed in favour of expediency.

**Issue 2: Recognition**

A critical factor in the addressing of privacy problems is the recognition that they exist.

In late 2002, this writer was unable to identify any long-term plan for the provision of an integrated privacy policy across a nationwide network carrying personal health records. No system had been designed to give individuals control of their personal health information. No steps were underway to identify such a system. Interviews with Ministry of Health information systems advisors failed to reveal evidence of any intention to investigate mechanisms by which specific control could be delivered to individuals, nor any insight that a privacy problem might exist. Instead, the information system leaders that were interviewed indicated that privacy measures applied by each of the multiple contributing network systems, such as at District Health Board level, would provide the required level of privacy.

This deficiency in planning and recognition is puzzling considering that:

- The various privacy principles have been well touted over the last decade.
- The 2001 New Zealand Health Strategy states: “Privacy and confidentiality of personal information must be maintained at all times in compliance with the Privacy Act 1993 and the Health Information Privacy Code 1994.”
- The WAVE report recommends the use of Privacy Impact Assessments to ensure that the framework indicated in the Privacy Act is achieved by the health information initiatives.
The Ministry appears to have been tardy in addressing these issues, which is regrettable in the light of the imperative to commence work early, as outlined in the preceding section. This tardiness may be explained by a preoccupation with the delivery of a few “quick fix” objectives, in an effort to justify the overall health information strategy.

**Issue 3: Control**

The WAVE report supports the Caldicott principles. The fourth of these principles states: “Access to patient-identifiable information should be strictly need-to-know”.

The question that arises is whether a health information system that follows the Caldicott principles should prevent individuals from accessing information unless they need to know it, or whether the system should merely ask individuals to refrain from accessing available records unless they need to know what is on them.

Existing information systems mostly work on the basis of authenticating the identity of a network user, then allocating that person permission to access information that is located within one or more section of the file system. In effect, each member of an authorized group is given a key to the filing room. They can then refer to any patient's file in the room, irrespective of the patient's wishes. Currently, the only thought given to information privacy is the notion that users of the system will be health personnel, either administrative staff or providers, and on this basis it is assumed that they will inevitably be beyond reproach. In an interconnected environment, those personnel could be located at any one of hundreds of sites across the country and even beyond these shores.

In an ideal world, an authorized health provider could access the resources of a network but would then only be able to inspect a specific patient's file if the patient hands the provider the key. This is the situation in which patients have true control over the privacy of their personal information.

In such a system, the advanced technology that currently threatens to erode personal privacy, can actually be used to deliver greater privacy than has ever previously existed. Provision of true control to health consumers requires that a whole new area of complexity be addressed. This would require the application of temporal and intellectual resources, in keeping with Issue 1 above.

**Issue 4: Trust.**

Interviews conducted by this writer have indicated that some prominent persons in various sectors of health care actually do not fully trust each other. In some cases these expressions relate to specific individuals, and in other cases they represent feelings of generic unease about whether it can safely be assumed that persons in positions of trust can and always will be trustworthy.

The same feelings of distrust may well exist amongst the general public. Arguably, the public will be reluctant to enroll in a system that can widely distribute their personal health records, without some serious guarantees, controls, and independent oversight.

**Finally:**

Individuals can only feel fully confident of their privacy if they can be assured that they
maintain control of their personal information.

Control is potentially eroded by increasingly complex computer systems, such as an interconnection of health networks. However, the technological sophistication that allows the development of internetworks could be used to improve privacy.

Different categories of health information carry different privacy requirements. For example:

- Some health information should be available to all people. This is likely to be in the form of non-identifiable statistics.

- A small volume of health information should be available to authorized persons without the permission of the individual. This is likely to be information related to an imminent threat to public safety.

- A small proportion of health information should be available to any authorized person, with the permission of the individual concerned. This is likely to relate to a very narrowly defined area of information, such as that contained on an immunization register, and information that would be critical in an emergency situation.

- Some health information should only be available to a specific authorized health provider with the explicit permission of the individual concerned. This is essentially all the individual’s personal health information that is not covered by the clauses above.

Each situation requires a different set of rules. For a system of health information to work, the public needs to be assured that all information has been allocated to the correct category, that each category of information has adequate privacy standards applied to it, and that all users adhere to those standards.

The essential elements for a system to handle personal electronic health information seem to be:

1. A system to guarantee the integrity, privacy and security of the data in storage and during transmission.

2. Verification of the identity of the health provider

3. Authorisation of the health provider to access that class of information, or to the relevant resources of the network.

4. Verification of the identity of the individual who owns the health information

5. Authorisation, by the individual, of the health provider to access that individual’s health information.

6. An active audit and review system to guarantee that the above system is followed.
New Zealand has the opportunity to lead the world in the development of an innovative ethical system for managing personal health records on a national level. The writer suspects, on current indications, that this opportunity will be neglected.