COLLATION OF MEDICAL RECORDS

Musings around the topic

Robert Stevens
Barrister and Privacy Consultant

In the excellent 2002 Nuffield Trust publication "Learning from Experience – Privacy and the Secondary Use of Data in Health Research" by Bill Lowrance, there is the following little apocryphal exchange between doctor and patient:

Doctor	Here, this medication will help your condition.
Patient	How do you know?
Doctor	A study of 10,000 people's experience showed that it helped 9,247 of them get better.
Patient	Good, I'll take it. But don't let anybody know whether I get better.

We have always recognised that health information about an individual, especially that collected or generated by a health practitioner in the course of giving advice and treatment, is special. The Hippocratic oath traditionally referred to such information as "sacred" in the hands of the medical practitioner.

There is another sense in which the privacy of health information is special, in that a feeling of autonomy is part of what we see as a healthy person - part of the goal of health care. And privacy is inextricably bound up with individual autonomy and feelings of self-worth. So to breach a patient's privacy is to prejudice their overall health.

However, it is undeniably true that medical research is hugely assisted by being able to study medical data on substantial numbers of individual patients, and it is almost as undeniably true that medical research has benefited and will continue to benefit humanity to the degree that there is a proper "public interest" in not just allowing, but positively encouraging it to flourish.

Moving on a few centuries from Hippocrates, what we now call a GP kept records on pieces of paper and card in a filing cabinet; the records about an individual were separate from those of other individuals, and they just happened to be housed together in the one cabinet, shelf or room. Similarly the hospital kept its own paper records, in the same manner. Security was very much a matter of physical controls upon access into the space where the records were kept. The records were not of much use to researchers because:

a) it was physically difficult to search through them, and
b) apart from a few very basic health facts, the data was not recorded in standardised form.

The records were really held for the assistance of the GP or hospital doctor, or their close colleagues and successors, for use in subsequent diagnosis and treatment. They may have had a secondary purpose in guarding against later allegations of misdiagnosis or mistreatment (certainly that reason is neither rare nor slow to emerge when it is suggested that records be destroyed).

Early medical research was carried out by individual doctors using their own patients and their own patient records. The idea of a researcher using records compiled by others arrived relatively recently.

Access to individual health data about numbers of individuals is useful – many would claim essential - for medical research which looks at a population as against an individual case. Most medical research which gets published today seems to be of this type. Such data is also useful for monitoring the incidence or association of certain health facts, whether for epidemiological medical research or for administrative or governmental purposes. Research and monitoring purposes are best served by individual health records being easy to search through, and containing data held in standardised forms.

There are administrative functions which impact upon health record keeping too. Once you get into systems of funding healthcare other than by the individual patient paying a fee for service, the funding body (whether private health insurer, government department, local funding authority, or even a major employer) is going to want details on what it pays for. Typically, the funding body will not expect direct access to the medical records, and may not need details at the level where a patient is individually identifiable at all, but they will almost always call for standardisation of diagnoses made and treatments provided. This need will sooner or later manifest itself in more standardisation of the patient records themselves, and will make the healthcare provider keep such records in a way which makes them part of an auditable administrative record system. Larger and more sophisticated funding bodies will dictate the format of administrative records maintained by the healthcare providers they fund and, as the detail demanded by a funding body increasingly calls for the sort of information previously held only in the individual clinical records, so the distinction between administrative and clinical data becomes less clear-cut and the healthcare provider is either required or at least motivated to use standardised medical software systems.

The sheer volume of health data generated expands enormously as a direct result of the advance of medical knowledge and technology – all those tests results - multiplied by the rising number of healthcare transactions in the population. All of this data has to be stored and be accessible. Fragmentation of healthcare among many more service providers means that each healthcare provider must be able to accommodate information received from other providers and must be able to produce data which can readily be transferred to other providers. It is probably these needs which drive today's healthcare provider towards the electronic health record held on a computer system, and it is probably the administrative elements of the healthcare provision processes which drive healthcare providers towards standardisation of formats and of glossaries for the content of the records.

Developing in parallel with these changes has been the demand for, and the capability of, linking health records compiled about the same individual by different healthcare providers or similar recorders of data. The old reliance upon the patient's name gives way to some digital system, encouraged in this change by the increasingly frequent need to match up one record with another easily, and by a secondary concern that records in transit might be more discreetly handled if referenced by something not instantly recognisable as a name. The expression of this change in New Zealand is the increased use of the NHI number, originally developed as an index to the location of paper records in the public hospital system and now used for a host of administrative functions.

Suddenly the old blocks upon the usefulness to researchers of individual health records held by individual healthcare providers are disappearing very fast: it is relatively easy to search through huge amounts of health record data, and that data is held in much more standardised forms. It is increasingly likely that the health records kept by different healthcare providers will not only be more accessible, and kept in standardised formats using recognised glossaries, but also that these records will include unique identifiers which can be used to link all those separate records which are actually about the same individual. More and more databases are being collated and maintained which have potential for new uses in research and monitoring, whether on an occasional or an ongoing basis.

This is the point that we have reached today.

For the different reasons mentioned above, quite independent of the need for research and monitoring bodies to access individual health data, that data is now on the very cusp of being hugely more accessible. The opposite side of that same coin is that the privacy of an individual's health information is now made much more vulnerable because more data is kept, more is collated or is at least 'interconnectable', and it is kept in standardised forms which are made very easy to access and to read.

One of the developments which has been mooted is the increased compilation of healthcare databases holding medical record information about individuals which has been obtained from several separate sources and combined using some linking and matching mechanism. Such databases can take many forms. We can see some early examples of that variety in New Zealand.

First, there is a collection of medical data held by the Royal College of General Practitioners, attached to the Medical School in Dunedin. It keeps data provided by many general practitioners about their current and past patients, and makes that data available to approved researchers on a tightly controlled basis. It has been operating for a number of years, but I understand that it has recently been expanded by the addition of secondary healthcare data from hospitals, matched to the original body of data by NHI number. Individual subjects of the health information held in that compilation may (or may not) have read a notice on the wall of the GP's waiting room to the effect that the practice does provide data to the College, but the extent to which that data is personally identifiable, and the coupling of that data with information coming in from the hospital system, is unlikely to have been made plain to anyone outside the medical profession. Wouldn't it be nice, and indeed reassuring, to pick up a leaflet in the doctor's waiting room as well as on a friendly internet site which describes how that database works, the controls upon access, and the more notable past and present research projects which make use of it? I don't know whether there is such a leaflet nowadays, or whether its production and distribution would be seen as a proper use of scarce resources, but I hope so.

A quite different sort of database was apparently being planned by North Health, a predecessor to the Auckland District Health Board, a few years ago. It was going to collect data on nearly all healthcare transactions which took place within its area, whether or not the transaction was directly funded by North Health, and collate that data using the NHI as the common unique identifier. There was some outline development of plans to control access to this ever-increasing database through a committee of worthy people who would consider each application. The plan was never announced publicly, and apparently faded away with the change in structures (and

names) of the HFA into RHAs into DHBs. However, there are still moves by bodies owned and controlled by the Ministry of Health, such as HealthPAC, to collect a lot of individual health data without explaining to the public why they are doing this. If your prescription carries your NHI number – and it probably does - then your pharmacist will be reporting the details to HealthPAC (whether or not the item prescribed is subsidised). It is, I understand, more likely than not that your GP is reporting to HealthPAC every visit you make there, including standard coding for the perceived reason for your visit, any diagnosis made by the doctor in relation to that visit, and any treatment given. This may well be happening even if your visit is not directly subsidised by the state at all. I hope that you been made aware of this disclosure and collation of health information about you.

The NHI itself is operated by New Zealand Health Information Services, an agency owned by the Ministry of Health. It makes your NHI number readily available to those in the healthcare business. It also keeps a record, against your NHI number, of all your hospital admissions and procedures, called the "National Minimum Data Set." This database was mentioned in a recent privacy case before the Human Rights Review Tribunal. A complainant had been misdiagnosed as a paranoid schizophrenic many years ago, later discovered this, and went to considerable lengths to get the medical records of the hospital and the doctors who had treated her corrected so that she would not be faced (again) by wrong assumptions that her symptoms of physical illness had a substantial mental element. In the course of getting those records eventually and properly updated, it was quite by chance that the woman learned of the existence of the National Minimum Data Set, where this old misdiagnosis was sitting in the NZHIS database accessible to any health care provider who bothered to look at it. That record was also corrected eventually but, had the woman herself not chanced upon its existence, it seems unlikely that anyone else would have directed her to it let alone taken steps themselves to have it corrected. The reason for this is that the National Minimum Data Set originated as simply an indicator of where paper files were to be located, it was set up in an age when there was no legal obligation to mention such things to individual patients, and its expansion over time to serve other purposes does not seem to have been matched by any effective new procedures to ensure that individuals are made properly aware of its existence and its functions.

All of these examples seem to be variants of the "trustworthy steward" type of scheme for safeguarding data confidentiality. To a lawyer, that seems particularly appropriate for safeguarding medical record information, which is generally obtained in the context of a form of fiduciary relationship (characterised by unequal power between the parties, and essential elements of trust placed by the weaker party in the stronger party).

It may confidently be predicted (as indeed it is by Bill Lowrance in the 2002 publication I quoted above) that:-

a) The scope and uses of health databases will continue to broaden;
b) Multipurpose databases will be used in the provision of care; in administration, payment, evaluation, audit, and planning; and in all sorts of research and public health work;
c) Distributed databases (i.e. networks) that collect data in intimate local detail but that can be queried as a whole will serve health research well;
d) "Sidestream" databases (i.e. *ad hoc* ongoing subsets of multipurpose databases) will be increasingly used and activated as needed;
e) The interlinking of databases will increase dramatically.

The question is whether, in the absence of effective central leadership or detailed regulation, adequate privacy can be preserved by the "trustworthy steward" model given the current mix of medical ethics, law and practicalities.

Since 1993 it has been a legal requirement in New Zealand that an agency collecting health information directly from an individual must take whatever steps are reasonable to ensure that the individual is aware of the collection and, among other things, the intended recipients of that information. If you ask the Ministry of Health how that legal obligation is being discharged when hospitals collect information which is going to be reported to the National Minimum Data Set, I think you'd be told (as I have been) that hospitals are meticulous in explaining such matters, including an option not to have the data so transferred. About three years ago I had an operation in a major public hospital. I wasn't told about any intended disclosures of information collected from me, and I was (more than most patients) attentively looking forward to hearing or reading just such an explanation. Was this just a rare oversight? I think not. During the same episode I was asked to sign a printed form giving formal, and presumably informed, consent to the administration of a general anaesthetic. I read the fine print on that form, and found that I would be signing to say amongst other things that I had received a copy of a certain leaflet about anaesthetics. I asked for a copy of that leaflet, which I hadn't seen. After a few hours I was told that the staff on the general surgical ward had never heard of the leaflet, let alone seen one, and that their enquiries revealed that it had not been used for many years, no copy could be found, and there was no current equivalent. In that environment, where they can't even get their paperwork remotely right to obtain informed consent for a general anaesthetic, does it seem likely that they are going to be assiduous about ensuring that patients are given knowledge and retain any measure of control in relation to the collection and dissemination of health information?

One can talk brightly about the technicalities of secure networks, about the craft of anonymising health data, about one-way data linking systems, and all of these things are well and good. But if the culture is not there among the workforce involved, such tools are not going to fashion the sort of security around health data which is necessary to earn and retain trust in any systems.

In Britain, the Caldicott Committee's 1997 Report on the Review of Patient-Identifiable Information recommended that "a senior person, preferably a health professional, should be nominated in each health organization, responsible for safeguarding the confidentiality of patient information." That sounds a little bit like our privacy officers, doesn't it? That "senior person" applying a set of broad principles also recommended by the Caldicott Committee, would be a sort of trusted steward too. Is that anything like enough to protect privacy in the face of this huge expansion in volume, in number of participants, in collation and interconnection, of individual health data? I think not. It is certainly fashionably "light-handed" as far as a privacy regulatory schemes go, and beguilingly cheap, but I suggest that it is almost unimaginable that it would achieve much at all unless there is also clear leadership on privacy within the health sector, and also quite detailed regulation embodying our undoubtedly worthy ethical and legal principles in such a way that anyone can apply them with confidence and consistency in practical everyday situations, check that they are applied, and detect and correct and perhaps even punish breaches.

You can take the light-handed approach where you have a culture which is strong and homogeneous in the relevant values, because it is enforced by peer-pressure. We are entering into a new age of health information handling. There are going to be many

more players, with many differing interests, and the information technology at their disposal gives them all more power to accumulate and disclose data on individuals but at the same time less chance of being observed in their activities by the individual subjects. Trust in the confidentiality of patient information is a foundation stone of health care as a profession, and the loss of that trust may well cause quite unexpected changes in patient behaviour which may harm health care itself. And trust of a profession may turn out to be quite fragile – easier to smash than to build. I believe it is unrealistic to expect sufficient homogeneity of privacy culture in tomorrow's health care operators for us to have confidence that light-handed application of broad privacy principles will be sure to retain that trust in the future.