Journal of International Information Management

Volume 8 | Issue 1 Article 3

1999

Managing health information in New Zealand: An analysis of the health information privacy principles

Felix B. Tan
The University of Auckland

Gehan Gunasekara
The University of Auckland

Managing health information in New Zealand: An analysis of the health information privacy principles

Felix B. Tan
Gehan Gunasekara
The University of Auckland

ABSTRACT

The New Zealand Health Information Service has recently established a national health register. At the heart of this development are three national databases. These applications and their functions are presented. Other initiatives currently being explored are also discussed.

The paper contends that these initiatives under the guise of advancing the nation's health may instead be infringing the privacy of the nation's citizens. An analysis of New Zealand's privacy legislation to the development of such a centralized health system is detailed. The paper concludes by considering the possibility of hidden agendas despite the provisions of the nation's privacy rules.

INTRODUCTION

There is a consensus in New Zealand's health sector that the existing systems and organizational arrangements do not meet current needs and will not easily accommodate the requirements of the health sector reforms and the information needs of the future. Fundamental changes to the organization of health services were then announced in the 1991 Health Information Strategy document. A significant component of this strategy is a framework for the development of health information services to meet the national requirements for health information.

This paper essentially describes recent developments in health information management in New Zealand initiated by the proposals in the 1991 Health Information Strategy. It discusses the role of the New Zealand Health Information Service (NZHIS) in the development of a national health register. It also considers the issue of privacy and confidentiality of the collection and use of health information. The paper argues that there is more than meets the eye. The government purports that a centralized health information management system should result in better health delivery by freeing up health resources (Ministry of Health, 1996), but at whose expense?

To set the scene, the paper begins with a background and an overview of the country's health information management. A review of the health information strategy initiative and a description of what has been implemented follows. A discussion of the issues around privacy and confidentiality ensures with special focus on the nation's privacy rules (Privacy Act, 1993a & Health Information Privacy Code, 1994). It concludes by questioning the real motives of the New Zealand Health Sector and its Government for developing a centralized health register. The paper suggests that to date the initiatives have failed to take into account and comply with New Zealand's stringent privacy principles.

HEALTH INFORMATION MANAGEMENT IN NEW ZEALAND

Up to and until the early 1990s, health information at a national level was provided and used by the then area health boards, private hospitals and the Department of Health (Ministry of Health, 1991). A review of the health information systems and related services then identified significant problems with the existing national collections and service. Some of these problems related to: (i) lack of quality standards and standard data definitions; (ii) problems of data accessibility and timeliness; (iii) uncoordinated and overlapping points of collection; and (iv) a poorly maintained National Master Patient Index. The review concluded that the current systems do not meet existing needs, neither are they able to accommodate the new requirements of the future, or the new requirements of the health sector reforms. A further conclusion was that new data systems, processing, and organizational structures are necessary to support the development of world class health care provision and management. There was a considerable consensus between, and within, working groups involved in the review on the need for change and the direction of that change.

In 1991, a national health information strategy was developed as a collaborative effort by the country's health sector (Ministry of Health, 1991). The strategy was designed to address the lack of relevant, timely, and accurate information. It provided a national framework for the development of health information services to meet the national requirements for health information. The strategy suggested the need to establish a new entity - the *National Health Information Service* - to manage the national health information services in New Zealand. This new entity, described in the next section, would streamline many of the current activities and manage the services as a business.

NEW ZEALAND HEALTH INFORMATION SERVICE

The New Zealand Health Information Service (NZHIS) is a group within the Ministry of Health responsible for the collection and dissemination of health-related information. It was set up in 1993 to implement the country's health information strategy. Its primary goal is to make accurate information readily available and accessible in a timely manner throughout the health sector. The NZHIS therefore has responsibility for all aspects of health information management - from the collection, processing, maintenance and distribution of health data and statistics to the continuing development and maintenance of a national health data and statistics to the continuing

development and maintenance of a national health information system, including the provision of appropriate databases, systems, and information products (NZHIS, 1997a). The vision of NZHIS is to support the health sector's ongoing effort to improve health information management in New Zealand. The NZHIS has recently established a national health register which may be the envy of many larger, wealthier countries (Sybase, 1998). The centralized repository of health information is summarized in the next section.

THE NATIONAL HEALTH REGISTER

The national health register consists of several core applications implemented on the Sun Microsystems platform with multi-CPU servers. Running over public electronic highways, these applications contain information for secondary and tertiary health events from Crown Health Enterprises (CHEs). At the heart of this development are three national databases: the National Health Index (NHI), the Medical Warnings System (MWS), and the National Minimum Data Set (NMDS). These have been designed to incorporate stringent safeguards to protect the information they hold from unauthorized access or misuse, but also to make crucial information about patients and their health available to authorized users for legitimate purposes.

National Health Index. The National Health Index (NHI) is a population-based register of all health care users (patients) in New Zealand. Assigned to each patient is a unique identifier allocated on a random basis. The NHI holds details such as names, alternate names, addresses, date of birth, gender, and ethnicity. This enables an individual to be positively and uniquely identified for the purposes of health care services and records. The NHI number is in fact not a number but a string of seven characters, the first three of which are letters and the last four are numbers. Details of the core fields which are recorded in the NHI database for an individual can be perused at NZHIS's on-line publication (http://www.nzhis.givt.nz/publications/NHI-MWS.html).

The NHI is developed essentially to help protect personally identifiable health data, particularly data held on computer systems, and to enable linkage between different information systems while still protecting privacy. Access to the NHI is therefore restricted to authorized users and is permitted by the Health Information Privacy Code 1994, under the Privacy Act 1993 (NZHIS, 1997b).

Medical Warnings System. The Medical Warnings System (MWS) is designed to "warn" health care providers of the presence of any known risk factors that may be important in making clinical decisions about individual patient care (e.g., allergies, sensitivities, past significant history, etc.). The MWS provides information on medical warnings and alerts, health care event summaries and donor information. These data are held nationally because of the clinical importance of quick access to the clinical information, and the relative geographic mobility of the New Zealand population. This enables a provider anywhere in the country to obtain potentially life-saving information about a specific patient in their care, once the patient has been uniquely identified. The responsibility for making sure that the content of the MWS is up to date will rest primarily with its users, the health care providers (NZHIS, 1997b).

National Minimum Dataset. The National Minimum Dataset (NMDS) is a single integrated collection of health data required at a national level for policy formulation and performance monitoring and evaluation. The NMDS provides a reliable, validated and comprehensive but selected set of information on: (i) the health status of the New Zealand population; (ii) the factors which influence health status; (iii) health resources and their utilization; (iv) the outputs, outcomes, and impact of health services for national policy making; and (iv) the performance of the health sector (NZHIS, 1997a).

The NHI, MWS, and NMDS are central to effective national health information management. In addition to these, the NZHIS also maintains a national cancer registry and records mental health events (NZHIS, 1997a). The NZ Cancer Register has operated since 1948 and is a population-based tumor register of all primary malignant disease. It is regarded as one of the oldest cancer registers in the world (Sybase, 1998). The mental health system is a register for all psychiatric patients currently in hospitals together with all admissions and discharges since 1974.

OTHER HEALTH INFORMATION MANAGEMENT INITIATIVES

Plans are now in place to expand the existing information base to include primary care information (NZHIS, 1997a). Considerable progress in this direction has been achieved, and various sites in primary care are operating with information systems that break new ground and offer significant advantages to patients, providers and purchasers. The use of electronic data interchange - for example, sending and receiving laboratory test orders and results or exchanging patient details for admission and discharge - is growing fast. Many provider groups are now making regular use of such facilities, or have pilot programs underway to explore their benefits. It will not be long before many of these programs coalesce into larger groups offering more services and therefore greater benefits to both doctors and their patients (NZHIS, 1997b).

Although the core function of the NZHIS is the management of health information for the Ministry of Health, it has also established a business center, offering its services on the open commercial market. The NZHIS has the flexibility to leverage its expertise to tender and bid for outside projects to generate additional revenue. An example of such external projects is the recent implementation of a pharmaceutical data warehouse. Funded by two commercial enterprises and in coordination with another agency responsible for managing pharmaceutical expenditure policy, the NZHIS was contacted to establish and store a data warehouse for all pharmaceutical information from across New Zealand (Sybase, 1998).

Every health care provider in New Zealand records and exchanges health information, and this is increasingly done in electronic format. The National Health Index (NHI) plays an important role in this process by providing a unique identifier for the whole health sector, including primary care. A wider use of the NHI would greatly improve the exchange of information between health care providers and make possible the integration of patient information from various sources. This can be facilitated by a Health Intranet (NZHIS, 1998). Pilot project are currently underway to develop a proof of concept. This will test the practical benefits of the Health

Intranet. When fully implemented, this initiative will provide a secure means of communications nationwide, with access to all health information systems for all health care providers registered to use the intranet.

ISSUES OF PRIVACY AND CONFIDENTIALITY

Most health information is collected in a situation of confidence and trust for the purposes of care and treatment. Assurances as to confidentiality and protection of privacy are vital components of the relationship between patient and health professional and are necessary if the latter is to obtain accurate information from the former in order to make an accurate diagnosis. It is therefore not surprising that the modern privacy rules overlap substantially with a much older law of confidentiality and the medical ethics of the profession. The notions of dignity and autonomy which underlie New Zealand's privacy law have also much in common with the idea of informed consent which is central to current medical practice (Slane, 1998a). Against this backdrop it is strange that there has been to date very little public outcry over the development of a centralized health register in this country. This can be explained by two possible reasons. Firstly, thee appears to be a lack of public awareness of the implications of these developments. According to a recent report prepared for the New Zealand Privacy Commissioner (Stevens, 1998), the issue of health information has bypassed public scrutiny. There are still many details to be addressed and debated. The lack of discussion involving all parties concerned has resulted in many doctors and even more patients being unaware of the type of patient details which are going to be collated and kept by health authorities. The same report goes as far as to suggest that there is something disquieting about the way health information is being managed in this country, with the health sector exhibiting a lack of openness about the various developments and plans in the collection of individual health information. As this program moves forward, it seems appropriate that more attention should be given to consultation with the public and debate within parliament. However, this is more than a matter of good public relations; it is a legal requirement of New Zealand's privacy regime that individuals about whom information is collected are informed as to the purposes of the collection as well as the intended recipients of it.

Secondly, it might be thought that there is a high level of acceptance and trust amongst New Zealanders that the information collected will be used appropriately. For instance, information can be used to catch people defrauding the system by matching data from various agencies like inland revenue, accident compensation and social welfare. Data matching is now a practice since the middle of 1998. Television commercials advising the public about interagency data matching serve as a warning about defrauding the government. According to a senior health official interviewed by the author, the general population appears to be comfortable with the concept of a health number for tracking hospital admission and discharge; the use of a universal number by general practitioners; and the recording of allergies and health history on a national database. For example, Community Service Cards were first issued in early 1990s and today around 50% of the population carry them. These cards entitle cardholders to discounted consultations with general practitioners, but they do not contain the NHI number or any medical infor-

mation. It appears that people are often surprised that these cards are not linked to their medical details and do not give their NHI number when swiped. An *improvement* to this card is currently underway in the form of a medical smart card pilot. The smart cards combine Community Service Card details, NHI number and medical warnings of the cardholder. New Zealanders have a strong history in accepting the use of electronic systems, with the highest penetration of EFTPOS terminals in the world (New Zealand Bankers Association, 1995). This may explain the high level of acceptance of the development of a centralized health information system and the use of electronic health cards in this country.

On the other hand, such acquiescence on the part of the general population cannot be assumed to exist. In the first place, while it is true that various data matching schemes between government departments exist (the Privacy Commissioner is empowered to sanction such schemes provided there are certain safeguards), the data matching schemes are targeted at what is perceived to be a minority anti-social element in the population. It is a very different thing to build up comprehensive health profiles of every single person, including law abiding citizens. Furthermore, reported complaints to the Privacy Commissioner provide evidence that ordinary citizens are particularly sensitive about their health information or about the potential misuse by health agencies of information about them.

In one case, for example, a customer complained when a pharmacy (where she was due to collect medicines which had earlier been out of stock) delivered medicines to her home without prior warning -- it was a case of the extra customer service not being appreciated. While a simple phone call would have avoided the problem an interesting question arises as to whether delivering medicines are directly connected with the pharmacist's purpose for holding the customer's name and address. Another complaint arose over the working of a form asking parents to consent to immunization. The form did not state how the information would be used. It also contained a number without explanation. The complainant assumed that children had been allocated identification numbers and that the information would be entered into a database. In fact the number was simply a batch coding for the vaccines, so that if something went wrong with one of the batches, the affected children could be contacted. Apart from statistical data, the main use of the information was in fact to inform the children's doctors so they would know whether to offer immunization. These cases show a keen awareness by members of the public of their right to privacy.

NEW ZEALAND'S PRIVACY REGIME

At first sight, New Zealand has a privacy regime which is well geared to the challenges posed by the development of a national health register. The Privacy Act of 1993 (the Act) is radical in its application as it applies to both the public and private sectors -- it applies to all "agencies" which are defined so widely that even individuals are subject to the Act. The Act governs the collection, use and disclosure of "personal information" (information about identifiable individuals). The Act also entitles individuals to access information held about them. Most importantly, the Act is *information* based, not *document* based. It does not therefore matter whether the information is stored or transferred through electronic means or through paper files - the same rules apply.

Central to the Act are the 12 Information Privacy Principles. For instance, Information Privacy Principle 1 (IPP 1) requires that only information necessary for a lawful purpose of the agency is collected and that the collection must be necessary for that purpose. However, this is also good information management practice. While the design of any data system proceeds backwards from the required outputs, one of the major health agencies recently put under scrutiny has been criticized because its outputs were evolving rather than having been stated at the outset (Stevens, 1998). IPP 3 is particularly important. It requires that an individual from whom information is collected is not only made aware of the fact of collection but also informed of the purposes for the collection and the intended recipients of the information. This most basic of requirements is evidently not always complied with especially when frontline health care providers are required to forward information about patients to central funding authorities (Slane, 1998a).

IPP 3 is relevant to Information Privacy Principles 10 and 11. IPP 10 requires that information held about an individual only be used for the purpose for which it was collected or for a directly related purpose. IPP 11 requires that personal information held by an agency not be disclosed outside that agency unless such disclosure is one of the purposes in connection with which the information was obtained, or is a directly related purpose. A crucial point here is that the purpose of the collection must be at the time of collection of the information. In other words, the purpose must have been communicated to the data subject (IPP 3). Otherwise, an agency could arbitrarily make up purposes for the information as it went along, or think of new uses for information it already has. This is contrary to the requirements of the Act. If the information is to be used or disclosed for purposes different to those articulated at the outset, consent must be sought from the individuals concerned.

One of New Zealand's major funding authorities (North Health) has been at the forefront of moves towards integrating primary health information (doctors and pharmacies) into its data depository. Through use of the NHI number the authority plans to collate and track individuals' attendance with different doctors, specialists, pharmacies, hospitals, and other clinics over the entire lifetime (Stevens, 1998). However, in brochures, encouraging the use of the NHI number no explanation was offered as to the information which would be collected through its use or as to the ultimate uses and recipients of it. More seriously, in terms of IPP 3, no purposes for the compilation of the information were clearly stated. It has been rightly pointed out that while the agency may have been merely seeking to gather as much information as it could while not yet having formulated uses for it, such an approach is anathema to the Privacy Act (Stevens, 1998). The end of this discussion will focus on the real motives for establishing centralized health information management and as to whether any of these goals are sanctioned by the privacy regime.

Other Information Privacy Principles are of significance for centralized health information management. IPP 5 is the only principle specifically addressing the security of storage of information. The Privacy Commissioner has observed that the focus of the Act is not only in stopping leads but in determining where the pipes lead (Slane, 1998b). IPP 8 requires that agencies take steps to ensure information is accurate prior to using it, a step which would seem especially relevant in the health context. IPP 9 requires that information be retained for no longer than necessary. Last, but not least, is IPP 12 which relates to unique identifiers. Among other things,

IPP 12 prohibits an agency from assigning, to an individual, the same unique identifier which has been assigned by another agency. It will shortly be seen that this last requirement has been specifically modified in relation to use of the NHI number.

It should also be noted briefly that the information privacy principles are, for the most part, not enforceable through the courts but rather through an alternative dispute resolution procedure beginning with the Privacy Commissioner (who acts in the first place as a conciliator) although a complaint can be taken to a tribunal which has considerable powers including the award of damages.

There are a number of qualifications and exceptions to the Information Privacy Principles. Some of these are stated within the principles themselves, for instance non-compliance for law enforcement and public health and safety purposes. Another common exception is where information is collected for research or statistical purposes provided it is to be published in a non-identifiable form. There are also grounds for denying access to personal information under IPP 6.

The principles generally provide that non-compliance may be authorized by the individual concerned. This has the potential to cause serious mischief, particularly when agencies regard consent as a panacea. There is always the tendency to regard a one-off consent as sufficient. Consent must be not only informed but genuine. In the health arena patients are at the receiving end of an unequal power relationship and the privacy Commissioner has referred to the "facade of patient control" (Slane, 1998b).

Finally, the Privacy Commissioner is empowered to modify the information privacy principles (by prescribing greater or lesser standards than contained in the principles) in relation to specified matters by issuing codes of practice which have the same force as the principles. This allows flexibility in adjusting the Act to the requirements of particular industries or types of information. Not surprisingly, one of the first codes of practice to be promulgated (there have so far been very few) was the Health Information Privacy Code 1994 (the Code) which is discussed next.

HEALTH INFORMATION PRIVACY CODE

In the introduction to the code three special characteristics of the health sector and health information are cited as the rationale for a separate code. These are: (1) confidentiality of collection (in the context of a confidential relationship); (2) the nature of the information (highly sensitive); and (3) ongoing use (health information may be required long after it has ceased to be needed for the original episode of care and treatment). It will be observed that of these the first two at least provide justification for more stringent standards than in the Act.

Despite this, the Code itself is an unremarkable document. The 12 Health Information Privacy Rules broadly follow the Information Privacy Principles. Perhaps the most useful feature is a detailed commentary which is no doubt useful to health professionals. There are some modifications of the privacy principles. From the point of view of the present discussion the most significant alteration is in Rule 12(3) which allows specified agencies to assign the NHI number

as a unique identifier. There are some safeguards. For instance, Rule 12(6) provides that an agency must not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned for a directly related purpose. However, as was observed earlier, it is extremely doubtful if these purposes have been communicated to the individuals concerned or indeed even articulated in the first place.

Rule 12(6) and it parent IPP 12(4) are seriously flawed for another reason. They do not preclude the unique identifier being obtained from someone other than the individual concerned. In the moves described earlier by the funding authorities towards building up a data depository one of the steps has been to require every claim for subsidy payments (most prescriptions and laboratory tests as well as some doctors visits are subsidized by the Government in New Zealand) to be accompanied by the NHI number of the patient concerned. It is easy to see how an otherwise reluctant profession can be coerced into supplying the number. Yet, a currently worded, they can be made to disclose the number for any purpose whatever.

The lack of adequate safeguards here is disappointing. When New Zealand's first privacy legislation was enacted in 1991, it served as a convenient smokescreen to allow the Government to proceed with plans for data matching. There is a danger that the Code will encourage similar complacency. Indeed it appears that the Health Ministry's statement in its web site that the Privacy Commissioner was involved in ensuring the highest standards of privacy were without foundation - the office had not even been consulted (Stevens, 1998).

HIDDEN AGENDAS

What are the possible motives or the rationale for centralized health information management? A number of possible explanations have been given (Stevens, 1998). No doubt the fundamental concern (in New Zealand as in other developed nations) has been to control the cost of health care to the government. One suggestion has been for "capitation" systems where individual customers are enrolled with a health management organization and identified each time they seek a health care service so that costs can be referred back to the responsible organization. If information is power, then an interesting application of a complete patient database is as a means of wresting power away from the doctors who are seen as currently accountable to nobody for their economic efficiency.

Another explanation has been that the new systems will eliminate or reduce the incidence of fraud (especially over state health care subsidy payments). However, these claims (for instance that as much as 11% of all claims are fraudulent) have been ridiculed -- if hundreds of millions of dollars were indeed being lost it is hard to explain why to date little or no efforts have been spent on audit and fraud detection. In any case it is extremely doubtful that the elimination of waste is covered by the gambit of the law enforcement exceptions to the privacy principles.

A more radical plan has been hinted at. This is to set up, for planning purposes, a database which records for every individual in New Zealand a substantial degree of detail about symptoms

as well as diagnoses and treatments (using a set of standard codes), and captures every health care transaction and the cost of that transaction whether or not it is state funded. Such a database would be a world first, and may well set New Zealand up as the world's foremost health research field and testbed. However, such lofty goals (even is they exist) have not been articulated at the level of the individuals concerned which, as explained earlier, is a clear violation of New Zealand's privacy regime.

Cogent reasons exist, on the other hand, for not relying on centralized medical records. In making diagnosis and treatment decisions, good medical practice suggests not trusting information recorded by others, especially where the accuracy of the information is vital. There is little or no empirical research linking better patient health outcomes with centralized medical records. Hence a full and accessible patient health record may not necessarily be beneficial to the patient.

Finally, the authors argue that a less benevolent possibility exists for the use of centralized health records. If the tentative steps taken so far in New Zealand eventually mature into a comprehensive centralized record for every individual then it will be possible to give every individual a classification as either a good, average, or bad health "risk." The utility of such information to insurance companies is obvious. It has been fashionable for some time, in New Zealand, to take an "insurer" view of health spending. There have been proposals for privatization and accompanying cuts in government health spending. One possibility which may be attractive to the government would be the "farming out" of certain patients to the private sector. The existence of a precise "risk assessment" mechanism will undoubtedly assist this process.

CONCLUSION

In summary, this article briefly outlines recent developments in health information management in New Zealand. A centralized national health register is now in place with a few thousand PCs linked to a central IT client/server platform. This system now services around 30 hospitals and other medical services providing health care to New Zealand's 3.6 million population. The resolution of a number of issues pertaining to individual privacy and medical ethics are the current challenges facing the nation.

While New Zealand possesses a highly developed body of privacy rules which clearly apply to the initiatives highlighted these are evidently not always complied with. The privacy rules mandate the fostering of greater public awareness of the uses of information. To date this has been lacking. It remains to be seen how effective the Privacy Commissioner will be in his potentially powerful role in monitoring and regulating the initiatives for centralized health information management.

REFERENCES

Ministry of Health. (1991). *Health information strategy for New Zealand.*

Ministry of Health. (1996). *Improving our health information system.* http://www.health.govt.nz/HIS2000/general/his2000_news.html.

New Zealand Bankers Association. (1995). *Annual review 1995.* Wellington.

NZHIS (1997a). *Data & services.* http://www.nzhis.govt.nz/projects/intranet.html.

Slane, B. (1998a, February 18). *Centralized databases: People, privacy and planning.* Paper presented by the Privacy Commissioner to the New Zealand-Australia Health IT Directors Meeting.

Slane, B. (1998b, July 15). *Informaiton protection in healthcare: Knowledge at what price?* Address by the Privacy Commissioner to the Health Summit '98,

Stevens, R. (1998, April). *Medical record databases: Just what you need?* Report for the Privacy Commissioner.

Sybase (1998). *NZHIS health register, 1st Quarter,* 16-17.