Report of a Privacy Impact Assessment

of a Proposal to Establish a Health Practitioner Index

Prepared for the Ministry of Health
by

John Edwards
Barrister and Solicitor

August 2004

A. Introduction and Overview

In October 2001 the Ministry of Health published "From Strategy to Reality – The *WAVE* Project"[1] ("the WAVE report"). The WAVE Report was the report of the WAVE Advisory Board to the Director-General of Health. The Board had been asked to "*facilitate the development, and acceptance by the health sector, of an Information Management and Technology Plan*".

The WAVE report set an overall strategic direction for the development of health information management and of health information systems. The Ministry of Health, particularly the business unit of the Ministry known as the New Zealand Health Information Service, has been engaged in scoping and implementing the recommendations of the WAVE report.

The recommendations of the WAVE Report were wide ranging, from common data exchange standards, to electronic health records, to integrated care, to the establishment of a health portal and knowledge management systems.

The development of a single numbering and reference system for health practitioners is a direct consequence of the process set in motion by the WAVE report, and was in fact ranked by the advisory board as the third of its top ten priorities.

This report is prepared according to guidelines issued by Office of the Privacy Commissioner and follows the format suggested in the Privacy Impact Assessment Handbook ("the Handbook")[2].

This report is intended to explain the proposal in plain language, and analyse the privacy issues from a policy perspective. This report is not a discussion of the extent to which (if any) the proposal can proceed in the existing regulatory environment. Analysis of the legal compliance issues is an important part of project planning, and has been undertaken. The Ministry had legal advice from Simpson Grierson in 2000 that a substantially similar project could take place in the legal environment existing at that time. The role of this report is to contribute to the debate around the questions, "given the privacy impacts (if any), *should* the project proceed", and if the answer to that question is "yes", "how can the project proceed in a way that minimises privacy impacts?"

A draft of this report was circulated to interested parties such as responsible authorities, and the Office of the Privacy Commissioner in April 2003. Since then there have been changes in the design of the proposed HPI and changes in the law. This version of the report reflects feedback received from stakeholders, the current design settings as at

[1] Ministry of Health "From Strategy to Reality – The *WAVE* Project Kia Hopu te Ngaru Health information Management and Technology Plan *Working to Add Value through E-information* October 2001

[2] *Privacy Impact Assessment Handbook* Office of the Privacy Commissioner 2002 p 17

December 2003, and changes to the law, particularly the Health Practitioners Competence Assurance Act 2003.

This report remains a "living document". As the project progress, further choices will be available to the system designers as to how the system is configured, what data will be collected, what technical security measures will be employed, who will have access to what information, for what purposes. At each of these decision points the privacy considerations should be taken into account, and made explicit in the decision making process.

Background to current data collection practices.

At present, providers of health and disability services are not identified in any standardised, uniform or coherent way across the health and disability sector. All the organisations with which providers must interact, including ACC, DHBs HealthPAC, Colleges and professional bodies all have different ways of identifying health practitioners.

A general practitioner for example might make a claim for payment of a general medical subsidy using the number assigned to her by HealthPAC and a claim to ACC using another number, they might order a laboratory test using a customer number allocated by the laboratory, interact with a DHB with yet another number, and be separately identified again to the Royal College of General Practitioners and the New Zealand Medical Association. Anecdotal evidence has some health professionals having up to 13 different numbers!

A single numbering system has the potential to make claims payment processes more efficient, and to make it easier for the institutions and the public to identify health practitioners, and determine their authorised areas of practice. The Ministry has been anxious to employ a national provider index system, or NPI (as it was then called) to achieve these aims since at least 1996[3].

A report prepared for the New Zealand Health Information Service in 2000 also noted:

> IPAs are groups of practitioners (mostly general practitioners) formed to provide members with common services. IPAs frequently have budget-holding accountability for certain services such as laboratory testing and prescription costs of their members.
>
> Presently, many IPAs are unable to properly account for the budget allocated to them in their contracts with funding agencies. The magnitude of these discrepancies is in some cases significant and has resulted in litigation between an IPA and the funder.
>
> The Independent Practitioners Association Council has endorsed the NPI as a mechanism which will assist IPAs to properly account for budget spending in areas such as consultations, prescriptions and laboratory tests. Support is also illustrated by the willingness of a number of IPAs to trial the use of the NPI and assist with establishing its adoption throughout the general practitioner community.[4]

---

[3] *Health Information Strategy for the Year 2000*, Ministry of Health, August 1996, page 23.

[4] *Privacy Impact Assessment National Provider Index Project* Simpson Grierson for the Ministry of Health 2000.
This report draws on the work produced as part of that report, and the contribution of Graeme Palmer, the author of that document, and others involved is acknowledged. Despite the fact that many of the privacy and policy issues were canvassed competently in that report, the Ministry has sought another report, primarily because of changes in the health sector and in legislation since that document was prepared. Rather than simply producing an update, the Ministry has sought in this paper a "stand alone" document. This in no way suggests that the earlier work was not acceptable to the Ministry either in the standard or in the conclusions it reached. However that report predated the WAVE Report, the New Zealand Public Health and Disability Act 2000, the Health Practitioners Competence Assurance Bill, policy and structural changes in the sector including the primary health strategy, and consequent reliance on primary

Description of the Project and Information Flows

General background

As discussed above, the 1996 document "Health Information Strategy for the Year 2000" established an action plan for the following five years with respect to the management of health information. A centralised standard means of identifying health practitioners was seen in that document to be an important part of the sector's ability to capitalise on new information technologies, for example by facilitating the electronic filing and payment of claims by health professionals.

A central registry and numbering system for health practitioners has been described as a critical feature of health sector information technology reforms in numerous reports over the last ten years, culminating in the recommendations of the WAVE report.

The WAVE Advisory Board described its top ten priorities for the health sector as:

1. Set up an independent organisation to lead IM/IT capability
2. Collect reliable ethnicity data
3. Implement the National Provider Index (NPI)
4. Fix up the National Health Index (NHI) - allow primary provider access, improve ethnicity data
5. Gather primary care information
6. Fix up pharmacy and laboratory data and provide primary care with access
7. Clean up messaging standards
8. Sort out Health Event Summaries - with data dictionaries, electronic discharges and referrals
9. Launch health portal
10. Make integrated care work by: developing standards for data exchange, security & network infrastructure

And … Involve patients!

In addition to the longstanding call for a central system of identifying health practitioners from a sector wide administration perspective, the Business Case for the HPI records a further imperative that is a factor of changes in the way health care services, particularly in primary health, are to be delivered and funded. The business case notes:[5]

> A key health sector strategic initiative is the development of PHOs and a shift to population based funding. To support the implementation of PHOs, key information infrastructure is required to provide details of practitioners, the PHO organisations and the facilities from which services are provided. This is critical to enable effective management of services provided by PHOs. The HPI will provide the unique identifiers required to accurately describe these details. Capitation payments require accurate information of practitioners, providers, the organisation they represent when providing a given service, and the facility from which the service is provided. Capitation requires mechanisms for provider and organisation "registration" and ongoing maintenance of this information in order to plan and manage contracts for provision of services.

---

health organisations and the bringing of claims and payments functions back inside the Ministry of Health.

[5] *Project Businesses case Health Practitioner Index Project* Peter King Peter Aagard, NZHIS 20 December 2002 at page 15

> Capitation requires the ability to identify when capitated providers obtain primary health care services from other providers, and when capitated providers provide services to non-enrolled individuals.

Some of the objectives of the HPI are to:

- Reduce transaction costs of health providers
- Ensure appropriate expenditure of public sector IM/IT funding
- Reduce compliance costs within the health sector
- Reduce duplication of investment in resource and technology
- Enhance a common purpose for IM/IT enabled sector improvement, and
- Ensure rapid progress in basic and fundamental issues[6]

It is proposed that the Ministry will obtain copies of the registers from registration authorities (called under the Health Practitioners Competence Assurance Act, which comes into effect in late 2004, "responsible authorities") which have a statutory responsibility to maintain public registers of health practitioners. The Ministry will configure this information into a database that allocates a single unique identifier to each practitioner. That number will be the practitioner's primary means of identifying himself/herself to health sector institutions.

In addition to its function as an "index", and source of a unique identifier, the HPI is also intended to be a single authoritative source of information about health practitioners for institutions such as ACC, DHBs, IPAs and the Ministry, and members of the public.

Limited practitioner information (such as updated address information) will also be obtained from other agencies, such as DHBs, ACC and that part of the Ministry of Health known as "HealthPAC".

It is proposed that the HPI will also assign a number to certain health sector workers (non-practitioners) who do not have any professional registration. For example, employees in a DHB who may require access to Ministry of Health information systems (such as the National Health Index) will in future need to have a number in order to log on to those systems. This is intended to provide a greater degree of security, and better audit capability, in respect of those systems. Although the information collected in respect of the non practitioners will be the same as for the registered practitioners, it is not proposed to give any third party access to that data.

Details have not yet been finalised and are likely to be influenced by this document, by consultation with responsible authorities, professional associations, and by public discussion, however it is likely that parts of the index will be open to public scrutiny.

Different levels of access for different users will be possible, however as it is anticipated that almost all of the information relating to practitioners will be derived from public registers. As such, practitioners might well have a reduced expectation of privacy in

[6] ibid p 15

relation to that information. Address information will not be part of public register, and as such will not be available for public search.

Examples of limitations that could be imposed, such as in respect of information that has not to date been treated as "public register" information, include authorisations to prescribe certain pharmaceuticals, or some restrictions on practice for disciplinary or competency reasons that have not been published.

Different levels of access can be designed to differentiate between individuals accessing their own information, access by the responsible agencies for their own purposes, by the Ministry for claims payment and research purposes, and by the general public.

Further discussion with the responsible authorities, and the professional associations will be undertaken before decisions are made on whether all members of the public will be able to have access to information originating from responsible authorities that has not, to date, been included on the public register (such as, in some cases, restrictions on practice after disciplinary proceedings), or generated by the funding agencies, (such as authorised to prescribe certain pharmaceuticals).

In areas where PHOs are responsible for administering budgets for primary health care, a PHO or DHB in that region might legitimately be given access to all the information about health practitioners in that region, but only a public access level to the remaining entries.

It is proposed that access is to be permitted remotely, probably over the internet, in much the same way as some responsible authorities already provide for public access to their registers.

Access to information derived from responsible authorities will be given only in accordance with the instructions of and agreements with those authorities. In other words the terms and conditions under which the responsible authorities will provide the register (and other) data to the Ministry for inclusion on the HPI will include limitations about who is entitled to view specified data fields. This will impose a considerable constraint on the Ministry's ability to arbitrarily change access rules.

In respect of non practitioners, there is no need to make the register information available to any third party. An employer for example might need to know that an employee has an HPI number, but will not need to know the data associated with that.

C. The privacy analysis

Introductory comments

It is estimated that approximately 200,000 New Zealanders will be directly affected by the HPI.[7] That number reflects the number of registered health professionals who will be assigned an HPI number, and whose data will be stored on the database.

This is a large number in a country with a total population of 4 million. The privacy issues involved in centrally recording and making public data about such a large number of individuals should not be underestimated. However it should also be borne in mind that the HPI project is not in itself responsible for all the privacy issues that arise. Many exist irrespective of the proposal. It is important that the consideration of the privacy issues involved with the project focus on, and make explicit the *incremental* privacy impact that the project is responsible for, rather than also adding in a discussion of the privacy affect of having all the information comprised in the various registers publicly available.

The privacy impacts of the HPI proposal can be summarised as follows;

1. Personal information currently made available through a number of different sources (http://www.mcnz.org.nz, www.dentalcouncil.org.nz, or in the public registers of the other responsible authorities), will be made available through one central point.
2. The HPI will collect and store some information not currently made routinely publicly available (for example information about practitioners generated by ACC and Pharmac, address information generated by responsible authorities or other claims and payment organisations).
3. The HPI will make information currently publicly available, more readily accessible to the public.
4. The HPI will assign a new unique identifier to health practitioners.
5. The HPI will assign a new unique identifier to other health sector workers.

These matters will be revisited in more detail below, however a very brief response to these general points might assist to focus discussion and debate;

1. **Personal information currently made available through a number of different sources will be made available through one central point.**
   The actual impact on privacy of gathering this information together in one place, and enabling a person to search it centrally is marginal. The impact on privacy of having information relating to all the different health practitioners searchable through one database will be restricted to practitioners registered with more than one responsible authority. For example, there is arguably a measure of privacy protection in the fact that it is necessary to search both the dentists, and the psychologists registers, to find out whether a certain named individual is

[7] ibid

registered as both a dentist and psychologist. Under the HPI a search on the individual's name may return both disciplines. Even in respect of this potential, it will be possible to design the system to prevent this marginal efficiency/privacy impact.

For example search fields can be designed to return results only from one discipline. If a consumer wants to check details of a clinician, but is not sure whether the clinician is a psychologist, a psychiatrist or a psychiatric nurse, the system could require each "register" to be searched separately, rather than simply searching across all the fields in the database on the clinician's name alone. This would preserve the current level of privacy protection through "inefficiency".

First mooted at the outset of the process of privacy impact assessment, the limitation of "one register at a time" searching has now been built into the design specifications, effectively neutralising the privacy impact of bringing the registers together in one place.

2. **The HPI will collect and store some information not currently made routinely publicly available.**
   Responsible authorities that are being asked to contribute their entire databases to the HPI may be concerned that information such as practitioners' personal contact details (eg home telephone number), which has never been made publicly available, may be included on the database. They can choose to not provide this field of data to the Ministry, or any such additional fields can be made subject to different access rules. Home telephone numbers for example might be suppressed so that they are not accessible via the public search part of the database.

   The need to differentiate between data for which there is a legitimate public need to retain in a publicly accessible form featured in the deliberations of the Health Committee which considered the Health Practitioners Competence Assurance Bill. The Committee recommended that address information not be part of the public register, even though responsible authorities might have legitimate reasons to collect that data. This recommendation was accepted by the House, and the Bill was passed with this amendment.

3. **The HPI will make information currently publicly available, more readily accessible to the public.**
   All the responsible authorities are obliged under statute to make certain information about the health practitioners subject to their regime, publicly available. This obligation is observed in a number of different ways, from internet access to an electronic register on one hand, to a book open to the public for search purposes on the other. It is arguably not a privacy impact to make information which must be publicly available, effectively publicly available. At the moment an Invercargill podiatrist may have a measure of privacy protection because her customers are not able to travel to Wellington to inspect the register of podiatrists. However this privacy protection is illusory, and the access right

discriminatory. The technical, physical and economic impediments to Invercargill residents obtaining access to the registration information arguably defeat the purpose of the public register provision. A Wellington resident can inspect the register and ascertain the details of local, Southland or East Coast podiatrists, regardless if he has any legitimate reason to do so. An Invercargill resident who can afford to, can ask a Wellington agent to search the register on her behalf and report the findings.

4. **The HPI will assign a new unique identifier to health practitioners**
   As will be discussed in greater detail below, the assignment of a new unique identifier, and its use by numerous agencies is a matter which does warrant close inspection from a privacy perspective. In this case the limitation of the identifier to the health providers, for use only in their capacity as such, will significantly reduce the potential for adverse privacy outcomes. The concept of common assignment for health sector purposes of a number assigned by a registration authority is already a feature of practice, and law in the sector. Rule 12(4) of the Health Information Privacy Code 1994 already permits such a practice.

5. **The HPI will assign a new unique identifier to other health sector workers**
   Expansion of a universal health worker numbering scheme is a potentially adverse privacy impact, and worthy of scrutiny. Such a step could be seen by privacy advocates as an example of "function creep", however it would not appear to be a significant step toward the main privacy concern in relation to unique identifiers, the establishment of a de facto universal national identifier. However, much work remains to be done on how the number will be assigned to non practitioners, the selection criteria for assignment, and the level of access to third parties anticipated. The extent to which the inclusion of non practitioners expands the privacy impact will depend on the outcome of that work.

Privacy is a key area of consideration in the development of the HPI, because it consists primarily of personal information about health practitioners. However, the privacy impacts of the proposal are not necessarily as significant as might at first appear. For various of the privacy issues identified there are likely to be process and technological solutions.

One of the most important features of this proposal which should give some comfort to health practitioners concerned about privacy, is that the Ministry must retain the trust and confidence of the responsible authorities.

The responsible authorities cannot be compelled by the Ministry to provide the information. Legal analysis indicates that the responsible authorities are not precluded by law from participating in the project, but they cannot be forced or required to provide the information for the database.

This means that if the practitioners believe that their privacy interests have not been adequately addressed in the design of the system, they can prevail upon their oversight agency, ie the responsible authority, to withdraw cooperation.

This should act as a very real constraint on any aspirations the Ministry has to treat the information other than with respect for privacy or according to clearly established agreed protocols.

i. Collecting and obtaining information

Information privacy principle 1

> Personal information shall not be collected by any agency unless--
> (a) The information is collected for a lawful purpose connected with a function or activity of the agency; and
> (b) The collection of the information is necessary for that purpose.

This is a principle of "minimum collection".

The HPI does not result in the collection of new information from individual health practitioners.

It does involve the collection of a greater amount of personal information by the Ministry of Health the professional record of 200,000 health practitioners. While much of the information at the moment is either available to the Ministry, or is collected by the Ministry in the course of processing payment claims, there will be information held on the HPI that the Ministry would not previously have routinely collected. For example, the records of a great many nurses will be recorded on the HPI where previously the Ministry might have collected information about only a very small proportion of the nursing labour force, in cases where it held contracts directly with practice nurses, nurse smear takers and so on.

The assignment of one number to each health practitioner has been identified as a key element in gaining efficiencies both for health practitioners and for central agencies. The Ministry of Health has the role and resources to undertake this task. As such it can clearly articulate a sufficient 'need', and a lawful purpose to collect the information.

Of the need to collect practitioners' addresses, the Ministry has said that that information must be centrally maintained to ensure clinical information is sent to the correct location, and for administrative reasons such as administering subsidised health claims. In addition the use of the information for workforce planning purposes (showing geographic distribution of practitioners) and showing members of the public who the practitioners in their area are have been cited as a justification for the capture and retention of address information.

Whether these reasons provide a sufficient justification for the central maintenance of addresses will be subject to further debate. One might well expect health agencies to

confirm address information directly with the intended recipient prior to despatching urgently required and sensitive information. One assumes that a relatively small proportion of all practitioners make direct claims for payment (for example many nurses are employed as staff in hospitals and surgeries and would not therefore be submitting claims for payment), and as such it might be difficult to justify holding address information about all practitioners. Workforce planning could arguably be achieved with geocodes or suburb/area name, rather than detailed address. As for informing the members of the public, the Yellow Pages appear to filling that purposes adequately at present.

Issues as to the accuracy, currency and ability to provide address information are discussed elsewhere in this paper.

These issues are likely to be simpler to resolve if the Ministry revises its need to collect address information. For example, the Ministry clearly has a legitimate purpose for collecting address information in the processing of claims (through HealthPAC), and would be entitled to store that information anywhere in the Ministry, including on the HPI. If the HPI address information was limited to address information obtained through HealthPAC, the privacy issues associated with address information would be much more manageable.

Information privacy principle 2

This rule relates to the need generally to collect personal information directly from the individual concerned and does not warrant detailed discussion in relation to the HPI.

The proposal offends the *principle* behind the rule, in that the information will always be collected by the Ministry from secondary sources (ie the responsible authority rather than the provider), but does not breach the law, which permits exceptions where compliance with the rule is not reasonably practicable, or where the information is publicly available, or where the individual concerned authorises the collection.

Information privacy principle 3

This rule requires openness between the primary collector of health information (ie the responsible authority) and the subject (the health practitioner) by specifying a number of things the collector must tell the subject about the proposed purposes for collecting the information and intended recipients.

It is incumbent on the responsible authority to advise the practitioner from whom it collects information of the intended recipients of the information, the purpose for which it is being collected, and to whom it will be disclosed.

The responsible authorities have been collecting the information that will be disclosed to the Ministry for the purposes of the HPI for many years, and in compliance with this principle must have been advising them that the information was to be retained on a publicly searchable register. It may be that the Ministry will be able to assist the

responsible authorities to amend their statements in a suitable way to comply with this principle in the light of the HPI.

One possibility for proceeding with the project that could be considered is to "stock" the database, and assign the identifiers only prospectively, so that individual health practitioners are all advised in advance of the proposal, and are able to make an informed choice as to whether on the basis of the proposed disclosures they renew their practicing certificates.

Such a step would remove any doubt for responsible authorities as to their legal ability to routinely provide the information to the Ministry. From the Ministry's perspective it would have a "cleaner" system, and would within the period of one registration cycle (ie 12 months) have all the information it is seeking.

ii. Use disclosure and retention of information

Information privacy principle 5

This principle requires that an agency holding personal information must ensure that adequate security safeguards are employed to ensure that the information is kept safe from unauthorised external access or internal misuse.

The fact that much of the personal information to be stored on the database is "publicly available", in no way diminishes the Ministry's obligations in respect of this section.

The fact that the information is to be centrally located, and remotely accessed increases considerably the security issues with the information as compared with the relatively decentralised status quo.

As the project develops and further choices become available to the designers of the system, the various ways of proceeding will need to be analysed from a privacy perspective. Some security issues which will need to be addressed, particularly if public access to the database is to be given over the Internet include:

- Different access rules for different accessing agents. For example individuals having access to the database over the internet will have more constraints than authorised institutions such as DHBs ACC, and the Ministry of Health. Those agencies will need to ensure they have adequate internal constraints to ensure that their access is not misused. Responsible authorities might have unfettered access to data relating to the professions they register, but only public access levels to all other data.
- The ability to reconfigure data to produce new combinations of personal information should be restricted, preferably to legitimate DHB and Ministry research, and there subject to rules relating to the further publication of such data. The system should not permit "mining" the data to produce for sale or hire, or

other commercial purposes information that would not otherwise have been available from the register[8].

- Public access over the Internet should be monitored to detect abuse, such as the attempted use of robots to obtain large volumes of data, and of browsing. For example, public search criteria could require at least two fields to be completed before a search can commence, name *and* region, or name *and* profession. Multiple returns could be limited to 5, and then only for the purposes of enabling the searcher to refine her search.
- Institutional access should be password or pass phrase protected and subject to restrictions and security standards that are contractually agreed in advance, and capable of being audited.
- There should be some means of suppressing from public search details where requested on reasonable grounds by the practitioner.

It should also be noted here that the HPI will contribute to an improvement in the security of other systems containing sensitive health information about consumers, in that the HPI number will be a means of authorising or limiting access, and providing a more ready audit capability to detect misuse.

Information privacy principles 6 and 7

These principles relate to the individual's rights of access to and correction of personal information.

There is nothing in the project which will adversely affect these rights. On the contrary, principle 7(4) provides:

> Where the agency has [corrected or added a statement to personal information at the request of the individual concerned on the basis that the information was inaccurate], the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

It might well be easier to give effect to this requirement under the HPI because it will be a central trusted source of information about practitioners. If inaccurate information is corrected once on the HPI it should no longer retain the capacity to adversely effect the individual concerned. Under the existing system, a practitioner might not have confidence that adverse information has been corrected in all relevant places once it has been dispersed. For example, a DHB or Ministry might have wrongly recorded an individual as no longer eligible to practice, perhaps because of a mistaken identity. Under the new system, once that error is corrected on the HPI, the whole health sector will see only the corrected information.

[8] Refer Public Register Privacy Principle 2, Privacy Act s.59, and discussion below at p 21.

Information privacy principle 8

Information privacy principle 8 provides:

> An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

The primary issue in respect of this principle is the timeliness of updates from each responsible authority. A regular update to detect not only new additions, but also changes to existing data will be required. It will not be sufficient for a responsible authority simply to advise the HPI of practitioners registered since the last update. Processes will need to be established to ensure that responsible authorities advise the HPI of changes of name or other data at frequent intervals to ensure that the database remains current.

One significant issue the project designers need to resolve before the project proceeds, is the relative currency, and accuracy of address information submitted by third parties. For example it is intended that DHBs, HealthPAC and ACC will be able to "update" the practitioners address field in the HPI. That data in the address field might have come from a responsible authority on Monday, and then HealthPAC notifies a more current address on Friday. There are dangers in assuming that the most recently notified address is the most accurate, or current. People may supply different addresses to different agencies for legitimate reasons. There are real privacy risks in substituting the more recent as the primary, or sole address.

In relation to address information it will also be necessary to have systems which enable the suppression of address information on the HPI, in circumstances where the individual concerned has asked that the information not be published. This issue is discussed further below.

Information privacy principle 9

This principle requires:

> An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

It is proposed that information will be retained indefinitely. This does raise a privacy concern.

In achieving its objective of ensuring people have only one number, and retaining information indefinitely, the system could have an adverse privacy effect as compared with the status quo.

For example under the current system, a nurse might allow her registration to lapse, and not renew her practicing certificate for some years. She might exercise her right under

section 28 of the Nurses Act (or s. 142 of the Health Practitioners Competence Assurance Act) be removed from the roll. These steps might even be taken partially out of a desire to protect her privacy. The HPI would need to retain her details, so that if in two years she reapplied for registration, she would still have her existing number. However, there would appear to be no reason for the details to be publicly available during that time.

Although not strictly a "retention" issue, but derived from it, the designers of the system should consider addressing this issue by providing search access both publicly and institutionally (except to the relevant responsible authority) only to "live", or current information, and to suppress the details of practitioners in respect of whom, in the absence of the number, would have been entitled to expect that their data would be deleted.

Information privacy principle 10

This principle imposes a constraint on uses to which personal information held by an agency may be put.

It does not preclude the Ministry from establishing the database, assigning a unique identifier, and then using that information and number for administration of claims, research and statistical analysis or other purposes.

The only constraint imposed is one that is set by the Ministry itself. It will be permitted to use the information for the purposes for which the information has been collected (from the responsible authorities and other sources).

Given the self definition involved, one may question what protection if any, this principle actually offers. However its value lies in the transparency involved in declaring the purpose for which the information has been collected. At the outset, the Ministry should impose clearly defined limitations on the permitted uses of the information. Any use consistent with this statement will be permitted. Any extension of the permitted uses should be subject to consultation with the responsible authorities and other groups who represent the interests of health practitioners, and subjected to further privacy impact assessment.

The management of information by a single provider number will enable agencies such as DHBs, PHOs or funders to make better use of information they already hold. This 'better use' might also have privacy implications.

It is important to draw a distinction here between a direct and indirect privacy impact of the proposal. At the moment, it might be difficult, although not impossible for ACC to know the average number of consultations for back injuries different physiotherapists provide, or for Pharmac to identify trends in pharmaceutical dispensing by any given pharmacist. The use of a unique identifier might facilitate the interrogation, or mining of their own data to ascertain if this information constitutes an efficiency, the absence of which may have in the past provided a measure of privacy protection.

The ability of those organisations to make such enquiries of their own data is not entirely dependent on the existence of an HPI, and would need to be conducted in accordance with the information privacy principles, and after due consideration of the privacy impacts of such reporting systems.

It is a question for further discussion and debate, whether an HPI should be resisted on the grounds that it will allow organisations to use the information they already hold in ways that will enable them to more efficiently achieve their business and policy objectives. Part of that further debate will be the extent to which the privacy interests warrant protection. The information at issue is after all, information about the business activities of health practitioners, rather than their personal lives, and relates to their claims for public funds.

Information privacy principle 11

As with principle 10, principle 11 allows an agency to self define the permitted disclosures. An agency that holds personal information should not disclose that information to another agency unless it believes on reasonable grounds that one of the exceptions applies. The exceptions include where the disclosure is:

- the purpose for which the information was obtained; or
- for a directly related purpose; or
- of information derived from a publicly available publication; or
- authorised by the individual concerned

There are no proposed patterns of disclosure proposed as part of the HPI that would breach this principle, and no issues relating to how disclosure might be effected which have not already been discussed in this paper, for example in relation to IPPs 3, and 5.

In the time that the project has been developed, the legal environment has changed in respect of at least one data item, practitioner address details. Under the Health Practitioners Competence Assurance Act 2003, a practitioner must advise the responsible authority of his or her postal address, residential address, and work address. The addresses do not form part of the public register, but the responsible authority can publish the address information as part of the public register if the practitioner has not objected in writing to the publication of address (sections 138, 140 and 149 of the HPCA refer). This represents a change from the situation as existed under the separate registration statutes (which will continue in force until September 2004), which made no provision for an opt out on the publication of address information.

It is now proposed that address information will not be obtained from responsible authorities, but from other sources such as HealthPAC. If, as is now intended, address information is kept separate from publicly searchable information, and subject to strict purpose based limitations on access by institutional users, the privacy issues will be mitigated.

iii. Assignment of Unique identifiers

Information privacy principle 12

This principle says:

> (1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any one or more of its functions efficiently.
>
> (2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of section 8 of the Income Tax Act 1976.
>
> (3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.
>
> (4) An agency shall 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 or for a purpose that is directly related to one of those purposes.

This principle has been amended in the health sector to enable the common assignment of numbers initially assigned by a responsible authority, Health Information Privacy Rule 12 (4) says:

> Notwithstanding subrule (2) any health agency, having given written notice to the Commissioner of its intention to do so, may assign, to a registered health professional, as a unique identifier, the registration number assigned to that individual by the relevant statutory registration body.

The extent to which the project can proceed under this rule has been considered by the Crown Law Office, which has advised that a formal code of practice amending IPP 12 is not required for the HPI to be able to lawfully assign numbers for further assignment and use by other agencies in the health sector.

The existing authority for multiple agencies to assign the same number applies only to health practitioners. In relation to non practitioners, it should be noted that it is possible for several agencies to *use* the same number without requiring special statutory authority or a code of practice. An inland revenue number is one example. It is assigned by IRD, and then obtained and used by employers, banks and others for purposes associated with the purpose for which the number was assigned. It would be a breach of the Act for a bank or employer to organise their customer or employee records based on that number.

Notwithstanding that the HPI can proceed under the existing law, in order to get at the actual impact on privacy it is necessary to understand the policy objective behind information privacy principle 12, and then to analyse the proposal with reference to this objective.

Dr Paul Roth of Otago University has attempted to classify the different objectives represented by IPP 12. His classification has been adopted, for descriptive purposes, by the Privacy Commissioner[9]. Dr Roth suggests four distinct features. They are summarised by the Privacy Commissioner as follows:

> *"Accuracy and use of personal information*
> Principle 12 is in response to concerns about the accuracy and use of personal information where a unique identifier is assigned. In particular, the risk is that if one unique identifier is used for a wide variety of authentication and identification purposes in both the public and private sectors this would amount to a de facto universal identifier. De facto universal identifiers have been viewed as unsatisfactory because they are unreliable and a threat to individual privacy.
>
> *Technical reliability*
> Because a de facto universal identifier is not designed to be a true universal identifier it can be technically unreliable and vulnerable to falsification or error.
>
> *Facilitation of privacy breaches*
> Any unique identifier that facilitates the exchange and matching of personal information held by different agencies and within different record systems is perceived to be a threat to privacy. This may also lead to the socially undesirable practice of compiling composite profiles of individuals which may lead to any and every aspect of their lives being open to potential scrutiny by governments or private enterprise.
>
> *National Identities by increments*
> The fear is that a de facto universal identifier emerging could ease the way towards a requirement of a national identity card or document. This brings with it a variety of concerns about inaccuracies and such like and the constraint on liberties. For some the idea of a national identity card is equated with mechanisms of a Police State where identification can only be authenticated and entitlements made on presentation of the card. Loss, lack or confiscation of such a card makes the individual a "non-person."

It is important to observe that none of these rationales for the regulations of unique identifiers point to any *inherent* privacy breach by the use of unique identifiers. This is significant. From this it might be surmised that from a policy perspective, it does not necessarily follow that the use of unique identifiers will result in a breach of privacy, in the same way as, say, the use of an information matching programme will.

The privacy breach is potential, and contingent upon subsequent uses of the number, and the technology supporting it. This point is underscored by The Privacy Commissioner of Canada. Commenting on a proposal to assign a unique identifier to medical student residents and physicians across Canada, he summarised his concerns in the following terms:

> " …. past experience has shown that personal information in an accessible form is subject to "function creep". Despite protections built into any system, the mere existence of the number will prompt creative and unrelated uses. Once all medical students and physicians are issued a number, there is a real likelihood of unauthorized access to their personal information using this number as the key. And when many organizations use any common identifier, the possibility increases that information from disparate sources will be combined into comprehensive profiles. Unique personal identifiers and

[9] Necessary and Desirable Privacy Act 1993 Review 1998 Office of the Privacy Commissioner p 88

> powerful technologies may appear to solve immediate administrative problems but they pose long-term threats to individuals' privacy, a fundamental value in a democratic society.[10]"

The assignment of a unique identifier here, and in Dr Roth's analysis is a stepping stone to negative privacy impacts, and may facilitate privacy unfriendly practices.

It is useful to consider the HPI proposal with reference to Dr Roth's categorisations, and the concerns expressed in Canada.

Unique identifier risks associated with the HPI

Privacy discussions internationally about unique identifiers are more often concerned with the dangers of individuals being assigned an official single number, or a number in common use being used as a de facto universal identifier.

Many jurisdictions have prohibitions on compulsory disclosure and use of unique identifiers other than for the strict purpose for which they were originally assigned. In Canada, the tax file number is protected in statute. In the United States rules apply to the use of the Social Security Number. The Senate Report for the 1974 Privacy Act (USA) noted that:

> "the extensive use of Social Security Numbers as universal identifiers in both the private and public sectors is "one of the most serious manifestations of privacy concerns in the Nation."[11]

Proposals for identity cards have not proceeded in New Zealand or Australia, because of privacy concerns. The anxiety engendered by the use of unique identifiers is largely because of the ability they give to accumulate and centralise information about an individual's dealings with the state.

The development of new sector specific identifiers with clearly defined purposes, as opposed to grafting on new applications to existing numbers can be seen to promote privacy by further embedding the fragmentation of information stores across the public sector.

The contrary position is put by the Canadian Privacy Commissioner in the example recorded above. In that case he expressed publicly his concern about a unique identifier that related only to physicians and medical students. It is relevant however that the disquiet he expressed was again based on the incremental and cumulative effect that such proposals have on privacy and the role of unique identifiers in becoming de facto identity systems.

---

[10] Privacy Commissioner of Canada Annual Report 1999/2000 http://www.privcom.gc.ca/information/ar/02_04_08_e.asp

[11] Privacy of Education Records David A. Banisar, *esq.* January 1994 Electronic Privacy Information Centre

The proposed HPI is not universal. If it were to be applied only to health practitioners and a limited class of non practitioners, selected according to clear "purpose oriented" criteria, the privacy risks could be limited. Although a large number of people would be assigned a number, the group is discrete. An identifier assigned to health practitioners could not readily 'creep' into other professions or sectors. Further, the information that is to be associated with the number is hardly likely to be 'intimate' or even details about the individual's 'private lives'. The information relates to the practitioners in their professional capacities, and in the most part is publicly available.

It is difficult to see what scope for extending the scheme to adverse privacy affect there would be.

It is clear from the foregoing paragraphs that much of the privacy concern is derived not from the limited proposal under consideration, but from potential extensions of the scheme.

Having considered potential privacy threats, it is necessary to consider how those threats may be mitigated, and what (if any) privacy gains might be made from the proposed system.

It is true that with a number it is possible to link data across organisations/ institutions. It is a privacy risk then that the number would enable records in respect of one GP to be linked across Pharmac, the Ministry of Health's claims and payment system, ACC's system, the responsible authority's competence and disciplinary system

Whether this is any more likely to occur in a way which intrudes on privacy under the HPI as opposed to the existing systems is moot. Moves in the sector to record all manner of personal information according to standard data sets and data descriptions would very likely lead to a greater capacity to share information across organisations and derive better information from organisations own data. The privacy *impact* of the HPI in a "but for" sense is therefore difficult to state with precision.

iv. Public register privacy principles

Section 59 of the Privacy Act sets out four public register privacy principles ("PRPPs"). They are:

> PRINCIPLE 1
>
> **Search references**
>
> Personal information shall be made available from a public register only by search references that are consistent with the manner in which the register is indexed or organised.
>
> PRINCIPLE 2
>
> **Use of information from public registers**
>
> Personal information obtained from a public register shall not be re-sorted, or combined with personal information obtained from any other public register, for the purpose of making available for valuable consideration personal information assembled in a form in which that personal information could not be obtained directly from the register.

PRINCIPLE 3

Electronic transmission of personal information from register

Personal information in a public register shall not be made available by means of electronic transmission, unless the purpose of the transmission is to make the information available to a member of the public who wishes to search the register.

PRINCIPLE 4

Charging for access to public register

Personal information shall be made available from a public register for no charge or for no more than a reasonable charge.

Principles 1, 3 and 4 apply to agencies which have statutory responsibility to maintain registers, and are subject to other laws authorising or requiring the registers to be managed in particular way. As such they are not strictly relevant to or binding on the Ministry, in the way it administers and gives access to the database.

The principles do reflect certain privacy values, and are an attempt to limit the privacy intrusion that public registers potentially represent. As far as possible, the principles should be taken into account in the design of the system. For example, permitted search variables should be specified in advance for the various levels of access. It may not be necessary to allow searching by reference to the HPI number in the public access, although such searches might be required by DHBs if DHBs are to let practitioners communicate with them only by reference to the HPI number.

Principle 2 applies to "any person", and as such will act as a constraint in the functionality the Ministry allows to be designed into the system. This principle appears to be oriented to limiting the commercial exploitation of databases that are made public for a legitimate public policy purpose. Some of the measures discussed above, in relation to IPP 5, will avoid breaches of this principle.

As far as possible, the HPI should be designed to limit the ability of users to recombine information for commercial purposes. This can be achieved through technical limitations on the search and reporting functions, and through the contractual arrangements with user institutions.

Precedent

International precedent

Canadians

The Canadians have developed a system very similar to that proposed for New Zealand. It is described as:

> The primary purpose of the Provider Registry is to uniquely identify each health provider across all jurisdictions, by assigning a unique lifetime identifier (the "Common Provider Number" or CPN). It should be noted that the Registry is not a repository of patient/provider encounter information, and will not include clinical data. It will be accessible by health sector stakeholders, by written agreement, and select data fields may be available to the public. [12]

[12] *WHIC Provider Registry Privacy Impact Assessment* HEALTHNET/BC *July 2001*.

Although developed by British Columbia to apply to doctors and nurses, the scheme was designed to be rolled out to other provinces, and with a capability and intention to add further provider groups.

The following description of the United States experience demonstrates some features in common with the drivers of the HPI system:

> **United States experience – provider identifiers**
>
> In 1993 the United States Health Care Financing Administration undertook to develop a national provider identification system to standardise and simplify the administrative burden of processing claims to health care programmes and plans. The Health Insurance Portability and Accountability Act 1996 ("HIPAA") includes provisions addressing the need for a standard unique health identifier for health care providers.[13]
>
> It was considered that the existing system placed unnecessary administrative costs on the exchange of healthcare related information and was unnecessarily complicated.
>
> Currently, in order to administer insurance and health care funding, the Department for Health and Human Services ("DHHS"), federal agencies, state Medicaid agencies and private health plans assign identification numbers to the providers of health care services with which they transact business.
>
> Each organisation assigns its own number to each provider and the subsequent lack of uniformity results in each provider having a different number for each program and often multiple numbers within a program[14]. The health plans are also required to co-ordinate with each other to ensure that correct payments are being made to the correct provider.
>
> As there are over one million providers in the US[15], the plethora of numbers creates enormous administrative difficulties, and errors in both identification and verification are common. Exchanging information is both expensive and difficult. As a result, a National Provider Identifier found significant favour among a very wide range of health care agencies, including state and federal agencies, insurance companies and professional and medical associations.
>
> The National Provider Identifier would be used to identify and validate providers. The provider information would be sourced from existing lists from professional associations. The number would be an eight digit number free of any embedded intelligence. Providers would use the number for all transactions for enrolment, eligibility enquiries, claim submissions, claim payments, remittance, managed care, outcome management, quality measurement, utilisation review, fraud detection, and benefit co-ordination.[16]

---

[13] Section 1173(b) *Unique Health Identifiers – (1) IN GENERAL - The Secretary shall adopt standards providing for a standard unique health identifier for each individual, employer, health plan , and health care provider for use in the health care system. In carrying out the preceding sentence for each health plan and health care provider, the Secretary shall take account of multiple uses for identifiers and multiple locations and speciality classifications for health care providers.*

[14] NPRM National Standard HealthCare Provider Identifier: Background Paper, http://aspe.os.dhhs.gov/admnsimp/nprm/npi01.htm

[15] NPRM National Standard HealthCare Provider Identifier: Implementation Paper, http://aspe.os.dhhs.gov/admnsimp/nprm/npi05.htm. This number is increasing by 30,000 each year.

[16] *Unique Identifiers for the Health Care Industry, Technical Advisory Group White Paper* October 1993, http://www.wedi.org/htdocs/resource/report/file 17.htm/

It is suggested that the NPI may be used:[17]

- by health care providers to identify themselves in health care transactions identified in the HIPAA or on related correspondence;
- by health care providers to identify other health care providers in health care transactions or on related correspondence;
- by health care providers on prescriptions (however, the NPI could not replace requirements for the Drug Enforcement Administration number or State license number);
- by health plans in their internal provider files to process transactions and communicate with health care providers;
- by health plans to co-ordinate benefits with other health plans;
- by health care clearinghouses in their internal files to create and process standard transactions and to communicate with health care providers and health plans;
- by electronic patient record systems to identify treating health care providers in patient medical records;
- by the Department of Health and Human Services to cross-reference health care providers in fraud and abuse files and other program integrity files;
- for any other lawful activity requiring individual identification of health care providers, including activities related to the Debt Collection Improvement Act of 1996 and the Balanced Budget Act of 1997.

The major issue for the DHHS is how and by whom the database is to be managed. The organisation responsible would allocate the numbers and maintain the database. The cost and structure of such an organisation is still under consideration.

It is intended that the integrity of the data will be controlled on three levels:[18]

- Error prevention: by building into the system adequate data edits and logic checks, and by setting pre-editing standards for organisations providing the data;
- Ongoing monitoring: tracking the consistency and validity of the data and resolving discrepancies resulting from the receipt of data from multiple sources;
- Active auditing: ensuring that the data is not just reasonable or logically possible but is also correct.

It is envisaged that certain information about individual providers will be protected. Access to the National Provider System (the complete database) would be restricted to the enumerators, those responsible for maintaining the database. The public would only be entitled to selected information.[19] [20]

For a more detailed description of the NPI visit http://cms.hhs.gov/hipaa/hipaa2/npi.pdf.

D.

[17] http://www.hcfa.gov.stats/npi/overview.htm
[18] Ibid.
[19] Ibid.
[20] supra Simpson Grierson Report

Privacy risk assessment

The various privacy risks of the proposal are set out in the preceding pages of this paper, and were summarised above as:

1. Personal information currently made available through a number of different sources (http://www.mcnz.org.nz, www.dentalcouncil.org.nz, or in the public registers of the other responsible authorities), will be made available through one central point.
2. The HPI will collect and store some information not currently made routinely publicly available (for example information about practitioners generated by ACC and Pharmac).
3. The HPI will make information currently publicly available, more readily accessible to the public.
4. The HPI will assign a new unique identifier to health practitioners.

The potential for these matters to constitute serious privacy intrusions is limited by the facts that much of the information is publicly available already, and also relates to the individuals' professional, rather than personal lives.

An assessment of net privacy risk requires a consideration of the potential or actual privacy gains from the proposal. Some of these may be summarised as follows;

· Single collection/verification

Each practitioner will provide one standard set of identifying information once, to the responsible authority. It will not be necessary for them to repeat that information to each institution with which that practitioner deals, thus eliminating the potential for errors and inconsistencies to creep in the recording of the information.

· Reduced transaction costs/claim payment time for health practitioners

While arguably not a privacy consideration, improved processing of claims will no doubt be appealing to practitioners. If a single reliable means of verifying identities for the payment of claims is available, the need for additional investigation, verification and collection of further information will be avoided, a more recognisable privacy benefit.

· Security of Transmission

Unique identifiers also enable the efficient and accurate transmittal of information about individuals, and can afford privacy protection, by sitting in the place of a name when the information is being processed or analysed. For research purposes, access to data can be obtained without identifying the research subjects, thereby protecting their privacy.

· Enhance security in other health sector information systems

There is real potential for the NHI number to contribute to added privacy protection for the consumers of health services, by adding a ready system of controlling and

monitoring access to other databases, such as patient record systems and the National Health Index. If a practitioner has to identify himself/herself with a unique identifier to obtain access to those systems, auditing of access and detection of improper access will be enhanced.

Much of the practical detail of the project remains to be examined, and will only be able to be assessed as the design stage progresses. The way in which the design stage progresses should be sensitive of privacy issues. The use of this document, and of the draft data provision and access agreements that have circulated to various interested parties should provide useful parameters on some of those design decisions. A further initiative, the development of a voluntary code of practice for all those involved in providing data to, maintaining or obtaining access to the HPI will also to assist to ensure that privacy considerations are not overlooked.