Privacy Commissioner
Te Mana Matapono Matatapu

Background Research Report on the National Health Index

April 2007

Table of Contents

As technological capacity advances, it is foreseeable that electronic health records will eventually become the norm for storing and sharing patient health information across various health care providers and facilities, as well as for those engaged in health system planning and research. While this trend has the potential to enhance patient care, it also brings with it the possible diminution of patient privacy.[1]

Introduction

Nearly every New Zealander has a National Health Index ("NHI") number, but only one in three knows that they do. This report has been prepared to provide some background on the National Health Index and its associated unique identifier. Its purpose is to inform and provide context for the Privacy Commissioner's proposed amendments to the Health Information Privacy Code ("HIPC").

Background

New Zealand's use of a national unique health identifier dates back to 1977. Initially this took the form of the National Master Patient Index ("NMPI"), which was held on a single mainframe computer system. The organisations responsible for maintaining this system were privatised and sold in the 1980s and 1990s. Since the move to a funder/provider split in the health sector and the associated break-up of Area Health Boards into competing Crown Health Enterprises meant that information would be held in separate independent repositories, the New Zealand Health Information Service ("NZHIS") was set up in 1992 to act as a centralised repository for key national standards and minimum data sets. To help it carry out this function the NZHIS established the National Health Index ("NHI").[2]

---

[1] University of Alberta, Health Law Institute Electronic Health Records and the *Personal Information Protection and Electronic Documents Act,* 2005, page 72

[2] For a summary of the changes and transitions in the New Zealand health sector, see Robin Gauld, *The Troubled History and Complex Landscape of Information Management and Technology in the New Zealand Health Sector*, 2006. It may be found at:

The NHI stores NHI numbers. The NHI number is a number/letter combination, assigned to each person using health or disability support services in New Zealand. A person's NHI number is stored along with his or her name, address, date of birth, sex, New Zealand resident status, ethnicity, date of death and a flag indicating any medical warnings or donor information stored in another system called the Medical Warnings System ("MWS"). The medical warning flag, which links to the MWS, is the only specifically clinical information stored on the NHI. The MWS is a long-running data-set, originally linked to the NMPI. The medical warnings incorporate adverse medical reactions and significant medical conditions; event summaries incorporate identification of the facility where the patient's medical record is held; and donor information incorporates donor summaries and healthcare user contact details.[3]

> *The core of the NHI is a database containing basic demographic information on individuals. Most of these data are held in a single table indexed according to a unique Healthcare User ID Number, more commonly referred to as the NHI number. External access to the database is controlled by software components known as Application Programming Interfaces (APIs) which execute the allowed transactions within the NHI, such as reading from the index, creating a new entry to the index and changing existing entries.*[4]

In an article outlining the history of the NHI, former NZHIS staff member Ray Delaney listed its three primary goals:

> ***Identification:*** *Different people with the same or similar names will have different NHI numbers, ensuring that the information pertaining to one does not get confused with that pertaining to the other.*

---

http://hcro.enigma.co.nz/website/index.cfm?fuseaction=articledisplay&FeatureID=020306.

[3] More information about the MWS may be found at http://www.nzhis.govt.nz/collections/collections-mws.html. A concise summary of the uses to which information on the NHI may be put can be found at http://www.nzhis.govt.nz/nhi/statement.html

[4] Delaney P, *Fourteen Years Young: A Review of the National Health Index in New Zealand* http://hcro.enigma.co.nz/website/index.cfm?fuseaction=articledisplay&FeatureID=020606

> ***Linking:*** *Data held about the same individual in many different databases can be brought together for the purposes of obtaining maximum information regarding a particular patient, as well as analysis and research.*
>
> ***Consistency:*** *When people change their names for any reason, the NHI number remains the same, thus ensuring longitudinal consistency with respect to information held about that person.* [5]

Access to the NHI and MWS is by direct electronic connection over the Health Intranet, via the National Health Index Online Access for Health ("NOAH"). Individuals and agencies wishing to access the NHI or MWS are obliged to sign a Deed of Agreement, which stipulates how NHI information is to be handled and what level of access to NHI or MWS is permitted for the users. The Agreement requires users to, among other things:

- Ensure that all information obtained from the NHI and MWS is used and disclosed solely for purposes contemplated in the Agreement and in a manner permitted by law;
- Comply with all reasonable directions and instructions issued by the Ministry in regards to access to the NHI and the MWS;
- Put in place procedures and policies to ensure the user's employees, contractors and agents are informed of their security and confidentiality obligations under the HIPC and Privacy Act;
- Ensure that only authorised employees, contractors and agents of the user who have a legitimate need to access health information are permitted access to the NHI and MWS;
- Use only approved security hardware and software to connect to NOAH;
- Ensure the accuracy, integrity and completeness of information supplied to the NHI and MWS.

The first item on this list is notable. Although the Agreement requires the user to ensure that information obtained from the NHI/MWS is used and disclosed "solely for purposes contemplated by [the] Agreement", no such purposes appear to be listed.

A further, important, requirement is that agencies signing the Agreement must be listed on Schedule 2 of the HIPC.

---

[5] Above note 4

Rule 12 and Schedule 2 of the HIPC

The NHI number is a unique identifier. Unique identifiers in the health sector are, largely, regulated by rule 12 of the HIPC.[6] Rule 12 is based on Principle 12 of the Privacy Act. Principle 12 prohibits agencies from assigning, for operational purposes, unique identifiers that have already been assigned by another agency.

> *Principle 12 may be seen historically as a response to concern which was perceived in early 1990s New Zealand that organisations (in both the public and private sectors) might increasingly use some common unique identifier to index their records, thus facilitating the interconnection of disparate items of information and the collation of dossiers about individuals. The spectre of the Identity Card was seen in the clouds and viewed with some alarm.*[7]

Rule 12 of the HIPC copies this prohibition, but provides an exception for agencies that both wish to assign the NHI, and are listed in Schedule 2 of the HIPC.[8]

"Assign", in this context, is something of a vexed term. It is not defined in the HIPC or the Privacy Act. A common reading of the term is that it means 'create a new identifier'. Another reading, and the one that has been preferred by the Office of the Privacy Commissioner, is that it means to affix an identifier to an agency's records as the single or main identifier by which the assigning agency will refer to the individual.

Accordingly, the NHI is effectively an *exception* to the general prohibition on the assignment of unique identifiers by multiple agencies. Schedule 2, which dictates which agencies are permitted to assign the NHI number, is a mix of large agencies (Ministry of Health, ACC) and smaller ones (Pathways Trust Board). Some of the agencies listed no longer exist, such as the Health Funding Authority.

---

[6] Health Information Privacy Code 1994, rule 12

[7] Stevens R, *Justice Sector Unique Identifier and the Definition of Assign,* unpublished memorandum used by permission of the author, 2001

[8] Health Information Privacy Code 1994, Rule 12(3)

Health information environment in NZ

The health sector, it has been noted, is 'awash with strategy documents'[9]. Major reviews were issued in 1991[10], 1996[11], 1999[12], 2000[13], 2001[14] and 2005[15].

The 1991 review identified problems with poor data quality, accessibility, uncoordinated systems and the poorly maintained nature of the NMPI. It recommended the creation of the NZHIS to provide access to health information for health agencies on a national level, as well as the creation of the NHI.

The 1996 Ministerial Strategy noted a lack of public understanding about the NHI and problems with the accuracy and completeness of information held on it. It recommended a focus on measurable population-based health improvement and identification of groups with poor health status, with the aim of improving services and making them more efficient. It also noted the fragmented nature of health information initiatives and concerns about the protection of privacy in the electronic environment, and recommended the creation of a national Health Information Council. This final recommendation was not implemented, possibly as a result of the amalgamation of the Regional Health Authorities into the Health Funding Authority ("HFA"), an absence.[16]

The 1999 Health Funding Authority Strategy reiterated many of the same concerns, including the need to "co-ordinate NHI use, formalise management of data collection and key health databases, create

---

[9] WAVE Advisory Board, *From strategy to reality: the WAVE project.* Wellington: Ministry of Health, 2001, page 15

[10] Williamson M, *Health information strategy for New Zealand: a joint venture between the area health boards and the department of health,* Wellington: Department of Health, 1991

[11] Shipley J, *Health information strategy for the Year 2000,* Wellington: Minister of Health, 1996

[12] Health Funding Authority, *Health funding authority strategic plan for information and technology management.* Wellington: Health Funding Authority; 1999

[13] Health Funding Authority and Ministry of Health, *Riding the wave: health information priorities.* Wellington: Health Funding Authority and Ministry of Health; 2000

[14] Above note 9

[15] Health Information Strategy Steering Committee, *Health information strategy for New Zealand.* Wellington: Ministry of Health; 2005

[16] Stevens R, *Medical Records Databases: Just What We Need?,* available at http://www.privacy.org.nz/library/medical-record-databases-just-what-you-need, 1999

formal processes for coordinating information and ICT development within the sector, focus on issues of quality and develop security and privacy guidelines".[17] While the 1999 HFA Strategy identified some 73 major projects to remedy business and information processes to improve or remedy these problems, a subsequent restructuring disrupted progress on them.

A report produced in 2000 as a collaboration between the Ministry of Health and the HFA recommended the creation of a set of national information systems based on individual anonymous patient data about health care events and that these systems should be accessible to all agencies managing population health.[18]

The Working to Add Value to E-Information Report ("WAVE Report") was issued in 2001 by the Health Information Management and Technology Plan Advisory Board. It reached many of the same conclusions as previous reports, observing the need for health care providers to be able to access patient and population information and service quality data and for the public to be able to obtain necessary information about procedures, comparative performance of service providers and their own rights and choices. One specific recommendation of note was for the establishment of two independent central organisations, one to lead policy development and one to continue with the maintenance of daily business transactions.

Common themes are apparent from these reports:

> *All found poor data quality, lack of standards, gaps in primary care data, accessibility and information exchange problems, a lack of co-ordination between data collections and systems and problems with national data systems and governance. Following such findings all made comparable recommendations.*[19]

Another issue that has been noted is the lack of public understanding, awareness and influence on the NHI/MWS and use of the NHI number.

> *Providers and consumers need to be informed about its purpose. This will enhance confidence providing those purposes are justifiable. Providers also need to be open*

[17] Above note 2
[18] Above note 13
[19] Above note 2

about the information to be linked by NHI number and the reasons. Adequate protections need to be in place to ensure its proper purpose.[20]

The government's current health information strategy is intended to "integrate" the health information sector and facilitate the sector-wide adoption of electronic health records to "enhance information portability and give patients greater access to their own information".[21]

As noted above, and partly as a result of the health restructuring of the 1990s, health providers have disparate and independent information systems. The prospect of creating a central monolithic health information database has been considered and rejected, leaving the intended course as one of uniting the multiple databases with a common set of protocols and processes. The NHI, as the national health identifier, is a crucial component of this project. The Health Practitioners Index (HPI) is also a vital part of plans to integrate the sector, but consideration of it is outside the scope of this paper.

Changes in the use of the NHI

In the mid 1990s there was a shift away from obtaining statistical information and towards providing transactional information to assist with managing service contracts.

One consequence of this was a drive to introduce the use of the NHI number into primary health care transactions. As a result, the protocols for management of the NHI, which had been designed around a relatively limited volume of transactions associated with people who made use of public hospital services, now needed to incorporate both a change in the nature of its transactions and a huge increase in the volume of transactions. The measures taken to achieve this were, in hindsight, quite inadequate.

Techniques such as pre-issuing a tranche of NHI numbers and mailing these to general practices on CDs resulted in a huge number of duplicate index entries being created. Payment of subsidies for general practice consultations were conditional on NHI numbers being embedded in the

[20] Above note 9, page 50
[21] Above note 2. See also below note 31.

subsidy claim, but there was no mechanism to ensure that the number provided matched the patient that was seen. Consequently, the level of confidence in the accuracy of the NHI, and its utility for primary care, plummeted.[22]

In a 2004 address the Chairman of the NZMA observed:

Epidemiological research, audit of healthcare programmes and health management analyses to determine health needs, evaluate health outcomes and allocated funding often rely on information derived from large numbers of patient records. Direct contact with the patients is not practical. It is generally in the patients' interests to be part of such a data collection, and in the public's interest to ensure the quality of these analyses.

However there is a tension here between the needs of epidemiologists and the ethics of clinicians. In making decisions about use of patient information we must ensure that pressures for efficiency do not result in the sacrifice of ethics.[23]

The Chairman's thoughts represent one way of using collated health information to provide, or improve the provision of, health services. However the tension he notes is an important one, as is that between the users and operators of the NHI and MWS system and the public whose information is being stored and used.

There are also, arguably, tensions between the needs of health administrators for workable and auditable record systems, the needs of health care providers for access to the right background information on the health history of an individual, the needs of researchers for longitudinal records they can access and analyse, and the wishes of the individual subject.

The subject may well prefer and expect total privacy, or at least a large measure of control over who sees what records about them. The incremental expansion of use of the NHI serves the first three interests in ways that can be largely unknown to the subject. That may, potentially, erode the individual's autonomy by creating a health information system of which the individual is unaware.

---

[22] Above note 4

[23] *Medical Ethics – Curly Questions,* available at http://www.conferenz.co.nz/medical-ethics-curly-questions.html

Other Perspectives

In 1998 the Privacy Commissioner issued a report examining plans to collate all health care transactions by way of the NHI ("the Stevens Report").[24] The Stevens Report examined the growing use of the NHI number as a global unique identifier in the health system and raised concerns over the way in which it was progressing, some of which paralleled those in the Delaney report.

> *Such interconnection and collation of health information may be very useful for the planning and co-ordination of health care, and may be of benefit to the individuals concerned, but this is not something which should be simply assumed without investigation and informed debate. The substantial changes to existing medical record systems will place a vast amount of additional information about the health care of identifiable individuals in the hands of various agencies which have not previously had such information in any useable form.*

The Stevens Report also highlighted the lack of opportunity for public debate, alleged coercion of health professionals and lack of co-ordination between agencies planning databases.

In 1999 Elisabeth Harding conducted a privacy impact assessment[25] ("the NHI PIA"). She reached the following conclusions, in abbreviated form:

1. A suitable policy framework for the management of identifiable health information existed but was not being adhered to;
2. Success of the framework was dependent on individuals and agencies 'buying in' to its aims and specifics;
3. Suppliers of NHI-associated information needed to be aware of the purposes for which it was to be used;
4. The use of the NHI number by the Health Funding Authority to monitor service agreements and report data to the Ministry was concerning;
5. Uncertainty about the use of the NHI was troubling, and was

---

[24] Above note 16

[25] Harding E, *Review of the National Health Index Number Privacy Considerations for NZHIS* 1999

contributing to a lack of cooperation across the sector and hindering the accuracy of the information collected; and

6. Administrative convenience needed to be balanced against potential privacy risks in using the NHI.

The review made 13 recommendations. Notable among these were that:

NZHIS should:

- Publicise the existence, purpose and operation of the NHI;
- Specify the purpose for which information obtained from the NHI could be used;
- Set up a procedure enabling people to find out their NHI number and facilitating personal access to, and correction of, information on the NHI by the people concerned;

Health Agencies should:

- Develop controls preventing the unauthorised linkage of information to the NHI; and
- Develop information management policies identifying the purposes for which they obtain information with NHI numbers attached. Policies should anticipate and document:
  - Legal authority;
  - Methods of collection;
  - Security safeguards;
  - Retention periods;
  - Procedures ensuring accuracy; and
  - Who may use the NHI number, for what purpose, what information would be attached to it

The report also recommended the setting up of a governance body to monitor the use of the NHI and the improving of the information held on it.

It identified the administrative, clinical and personal benefits as being:

1 Information may be communicated without attaching a name;
2 Simplification of administrative tasks;
3 Standardisation of unique identification numbers within the health sector;
4 Facilitation of the collection of information for national statistical purposes;
5 Easier detection of fraud;
6 Improved accuracy of information;

7 Easier transfer of information;
8 Improved linkages of information.

The report noted the need for an 'effective unique health identification system' to balance these benefits with policies specifying who may use the identifier and for what purpose, as well as creating policies preventing the unauthorised linking of information by the unique identifier.

Many, if not all, of the benefits identified in Ms Harding's review relate to the creation of an electronic health record, and it may be useful to consider this more closely.

Electronic Health Record

An Electronic Health Record ("EHR") is[26]:

> *An electronic longitudinal collection of personal health information, usually based on the individual, entered or accepted by health care providers, which can be distributed over a number of sites or aggregated at a particular source. The information is organised primarily to support continuing, efficient and quality health care. The record is under the control of the consumer and is to be stored and transmitted securely.*

The requirements for implementing EHRs have been cited as including:

1 *Consumer*
2 *Regional systems required by the DHBs and hospitals*
3 *Community and local systems*
4 *National connectivity and access*
5 *Core national systems such as the National Health Index, Practitioner Index, National Minimum Dataset (Inpatient) etc*[27]

In the report cited above, the author suggested the benefits of EHRs

[26]Australian Department of Health and Aged Care, *A Health Information Network for Australia: National Electronic Health Records Taskforce Report,* Canberra: 2000
[27] Kerr K, *The Electronic Health Record in New Zealand*, 2004, available at http://hcro.enigma.co.nz/website/index.cfm?fuseaction=articledisplay&FeatureID=040304

as being improved[28]:

- Coordination and quality of health care;
- Clinical decision making support functions;
- Access to clinical data, aggregated at regional and national level;
- Prescription costs.

The primary benefit of creating and maintaining a system of electronic health records is generally stated as being to improve the delivery of health services. The 2000 Australian National Electronic Health Records Taskforce report also suggests that a central benefit of EHRs is that health consumers will benefit from better and faster access to their own records.[29] This does not appear to be a primary goal of New Zealand efforts in this direction. The NZ Health Information Strategy for 2005 (HISNZ) lists "consumer involvement – increasingly consumers wish to make informed decisions about their own care and would like easy access to knowledge"[30] as a "global trend in health information systems" but only tangentially mentions it as a desirable result of projected New Zealand developments.[31]

Concerns are noted as including the privacy of the information shared and held, and a dilution of the doctor-patient relationship, as well as the time and expense of setting up systems and training clinical staff to use them.

> *Further, very clear guidelines and a strong national data governance framework would be required for EHRs to be successful.*[32]

The NHI is a key component in the creation of a national EHR, as noted in the HISNZ:

> *Various forms of EHRs are used to convey clinical information, as well as to coordinate care for particular diseases or services. There is growing recognition of the*

---

[28] Above note 27
[29] Above note 26
[30] Above note 15, 2.3
[31] The Health Information Strategy Action Committee (HISAC) is responsible for the development and implementation of HISNZ. HISAC terms of reference allow for a consumer representative to be appointed, and it is currently assessing the feasibility of doing this. Also, consumer representatives have been appointed to the HISAC National Collections Sub-Committee.
[32] Above note 26

need for common 'anchors', such as unique identifiers that enable EHRs to span the continuum of care.[33]

The report goes on to note:

Despite early promises, there is an emerging realisation that a single integrated record is neither workable nor practicable. Most countries are seeking to link multiple pockets of electronic health information into some sensible formation to help provide better and safer care.

EHRs are recognised as a virtual concept that relies on a network approach, where data is pulled together from multiple data stores. It is no longer viewed as a single physical repository.[34]

Developments in the United Kingdom have been moving along similar lines, with the National Health Service resiling from plans to compel all health information about UK citizens to be stored on a central database[35] and acknowledging that plans to build a single monolithic database for storing information relating to its new ID card were impractical.[36]

The creation of a national EHR presents significant technical problems as well, particularly in terms of standards for syntactical methods needed to encode medical information in a machine-readable format.[37] New Zealand's use and widespread adoption of the NHI has been cited as constituting a significant advantage in the creation of a national EHR:

In summary the decision by the NZ Government in the early 1990s to invest in and promote key items of health information management infrastructure [including the NHI] has positioned it as a world leader in the field, particularly in the primary care sector.[38]

---

[33] Above note 26
[34] Above note 15
[35] http://society.guardian.co.uk/e-public/story/0,,1974600,00.html
[36] CardTechnology, *UK Details Plans For National ID Smart Card*, 22 December 2006, available at http://www.cardtechnology.com/article.html?id=20061219IX4CKCL5
[37] The two market leaders currently are HL7 and Snomed. A description of HL7 by its creators can be found at http://www.hl7.org/about/, and the equivalent entry for Snomed is at http://www.snomed.org/snomedct/index.html.
[38] Above note 26

New Zealand's small size and the high level of technical uptake among medical professionals appear likely to make the implementation of a national EHR easier and more practical by international standards.[39]

Example: PrISM

In late 2005 West Coast DHB completed its implementation of a system called Primary integration Systems Management ("PrISM") to link primary and secondary care along the West Coast, using telecommunications infrastructure laid down by the Ministry of Education as part of a broadband in schools initiative.

All of these systems share a common index (based on the NHI) and will eventually be integrated with one another. Adding in electronic ordering, electronic discharge summaries and electronic referrals, is intended to lead to the formation of a single shared electronic health record for the West Coast population. Each of these systems can be accessed from any location on the West Coast DHBs wide area network and can be made available to other DHBs through the South Island regional shared "One Office" network.

> *The West Coast DHBs wide area network (brought about by the PrISM system) already connects to all of the West Coast DHBs primary health clinics except of Haast (due to technical limitations of current satellite technology). This system will be made available to all independent primary health providers on the West Coast, so as to become a whole of West Coast health information network, which is already linked to the South Island regional DHB network. Connecting the South Island Network to other regional networks is all that is required in order to achieve a National Health Information Network that includes the West Coast.*

Information is stored centrally and accessed by PHOs along the West Coast.

---

[39] See also this list of desirable characteristics for a health unique identifier, nearly all of which apply to the NHI: http://hcro.enigma.co.nz/website/index.cfm?fuseaction=articledisplay&FeatureID=020606#7

All of the West Coast DHBs systems use patient NHI numbers as the main index field in their database tables. Primary Health providers on the PrISM system use the NHI as their unique patient identifier, for example. The West Coast DHB is a leader on uptake of the NHI system and has rigorous checking and auditing processes in place to limit the risk of duplication of NHI records.[40]

The West Coast DHB plans to expand its coverage to include dental services and Maori Health Providers, as well as all primary healthcare providers in the area. In a presentation at the 2006 HINZ conference, the CIO for Southland DHB noted the advantages of PrISM as being: [41]

- *A number of sites that weren't previously computerised now are;*
- *All data is stored centrally; data never leaves the WCDHBs internal IT network;*
- *All data is backed up and we test that it can be restored;*
- *If someone steals a PC from a remote clinic, there's no data on it;*
- *Any user in any location can be given access to any information from any of the WCDHBs systems but will only be given access when it is appropriate for them to have it;*
- *All of the WCDHBs systems are being integrated so as to create a complete Electronic Health Record.*

PrISM is one possible model for New Zealand development of the shared EHR. However, it is important to note that PrISM is not an example of the decentralised model outlined in HISNZ. PrISM was introduced, at least partly, to address the high percentage of West Coast GPs who do not have electronic patient management systems. Systems of this nature are widespread throughout the rest of the country, making a centralised system like PrISM unnecessary.[42] Future national health information systems are focused on using a decentralised approach, keeping data at its source and only passing on aggregated data as necessary.

---

[40] West Coast DHB, *District Annual Plan 2006/2007*, available at http://www.westcoastdhb.org.nz/publications/reports/annualreports/pdfs/dap2006.pdf

[41] A copy of the slides from the presentation may be found at http://www.hinz.org.nz/media/2006_conference/2006ConferencePDFS/DHB%20CIOs%20Open%20Forum.pdf

[42] Information provided by Ministry of Health staff, 4 April 2007.

Privacy and Compliance

A recent American survey indicated that, while 48% of US consumers saw benefits from having an EHR, around 70% expressed one or more concerns about possible negative effects. Significantly, the most commonly expressed concern was that medical information might be shared without their knowledge.[43] There are two aspects to the NHI which are relevant to this concern. The first is that a unique identifier such as the NHI makes it easier to link disparate data sets, thus potentially allowing a single data item to be the 'key' to a range of intrusively personal information. This is particularly problematic when the unique identifier has more of the characteristics of a 'name' than of a 'password'. The second aspect is that the absence of a unique identifier means that a range of other personally identifiable information must be used in its place, such as name, address, occupation and date of birth.

Names vs passwords

The privacy considerations around unique identifiers mainly relate to the ease with which disparate data sets may be merged, using a unique identifier, and the way this can result in information being used for purposes other than those for which the information was collected.

However, David Brin's distinction, in *The Transparent Society,* between a *password* and a *name* is also of interest. In the context of the US Social Security Number ("SSN"), Brin observes that it has all the characteristics of a name, but was treated like a password. This had multiple consequences for security and safety of personal information associated with that identifier[44].

> *The contrast between a name and a password goes to the core of many modern privacy problems and their potential solutions. Names are what help keep people accountable. They should not enable others to harm you. Names verify the fact that a transaction is taking place, which is a*

[43] Givens, *Medical Records Privacy: Fears and Expectations of Patients,* available at http://www.privacyrights.org/ar/speech2.htm, 1996
[44] Brin D, *The Transparent Society*, 1998, chapter 8

completely separate matter from giving permission for the transaction to proceed. Names are inherently open things. We base countless decisions on having fair knowledge about the reputations of others – whether they are skillful, credible, or reliable, for instance. On the other hand, passwords set transactions in motion. They require secrecy.

Brin's distinction can be of assistance in considering whether a particular unique identifier is harmful or helpful to the privacy of the person concerned. The NHI number has certain characteristics in common with the SSN, in that it is a well-established unique identifier associated with the great majority of the population. It differs in that

- Its use is effectively restricted by rule 12 of the HIPC to the health sector;
- Most individuals are not aware of their own number or even that one has been assigned to them; and
- It is rarely (if ever) used as an authentication method.

In terms of Brin's name/password distinction the NHI number is clearly better suited to be a name rather than a password. Some difficulties may arise from the use of the NHI as a sole identifier, such that it is *required* for access by a health practitioner to a particular set of health records held by a DHB or other health agency.

It is possible the mere fact that someone has access to a given NHI number might be taken, mistakenly, as indicating he or she has a higher right of access to the information associated with that number than is the case. Robust information systems security and processes can, and should, provide a privacy protective barrier against this form of attack.

Privacy implications of the NHI

Some of the NHI's apparent functions are to:

1. Help improve care by ensuring medical information is associated with the correct person;
2. Improve ability for identifiable health information to be transferred without using the names of information subjects;
3. Act as a central repository of information for use in research; and

4 Provide a framework for EHRs.

Of these, items 1 and 2 are potentially privacy friendly. Items 3 and 4 are, at best, neutral and possibly privacy hostile.

Complaints

A search of OPC complaints files reveals 23 complaints which make some reference to the NHI between 1998 and 2006.[45] Over that period the Office received a *total* of around 10,000 complaints. Only two complaints were received alleging a breach of rule 12, and in neither of these cases did the Commissioner form the view that an interference with privacy had occurred.[46]

The low proportion of NHI related complaints might be taken as indicating a lack of knowledge or lack of concern by individuals about the NHI, or alternatively that use of the NHI by health agencies is, largely, compliant with rule 12.

A representative sample of these complaints is as follows:

- Complaint that NHI number assigned and health professionals given access to information stored under number without patient's knowledge or consent (1998)
- Investigation into the storage of information relating to Guthrie Card Tests (2000)
- Request for access to health information held by funding organisation (2000)
- Theft of patient notes, indexed by NHI, from laptop being used for research (2002)
- Use by ACC of complainant's NHI without consent (2004)
- Retention of NHI number by Cervical Screening Program against wishes of complainant (2005)
- Collection by landlord of complainant's NHI number (2005)

[45] Search undertaken by the author on 14 December 2006
[46] Search undertaken by the author on 18 December 2006

Themes that can be discerned, despite the small sample size, are:

- Concerns over security;
- Collection, assignment or retention without consent; and
- Access, whether authorised or not.

The NHI number, as a health unique identifier, is regulated by rule 12 of the HIPC. Although rule 12 is the only rule which specifically mentions the NHI number, it is not the only part of the HIPC that is relevant. For example privacy concerns may potentially arise about the use of the NHI, not in relation to the Index itself, but rather about the use of the NHI number as a unique identifier tying together disparate data sets. Accordingly the other rules of the HIPC are all relevant, and are considered below.

HIPC Rules and the NHI

Rule 1

Rule 1 requires agencies to have a lawful purpose for the collection of health information and for the collection of that health information to be necessary for that purpose. The collection of an NHI will normally take place in two circumstances, the first when it is collected directly from the individual to whom it relates, the second when it is collected from another health agency.

Collection from the individual

As noted above, understanding of the existence and purpose of the NHI is not widespread among the general public. Although an estimated 98% of New Zealanders have had NHI numbers assigned to them, few are aware that this is the case. Accordingly collection of the NHI directly from an individual would be less common than with many other commonly used unique identifiers such as the driver's licence number, passport number or IRD number, simply because it is unlikely the individual will be aware of, let alone know his or her number.

Collection from a third party

Where the NHI number is collected from another agency, the purpose for which it is collected will normally be associated with the provision

of health care to the individual concerned. Other purposes for collection include the auditing of health services provided and securing of funding for those services. While rule 1 requires an agency to have a lawful purpose for collecting health information, it does not require any transparency about this purpose.

Rule 2

Rule 2 requires the direct collection of health information except where one of the exceptions to the rule applies.

The NHI number is often, indeed almost always, *collected* indirectly after being *assigned* by one or more health agencies. In a strict sense, this can mean that the individual:

1. May not be aware of the collection,
2. May not have had the chance to have the purpose of the collection and possible destination of the information explained, and
3. May not been given a chance to refuse to authorise the collection.

Despite this, since most people do not know their NHI number, it will often be not practicable to require agencies to obtain it directly. Because of this it is probable that the collection from a third party does not breach rule 2 of the Code.

Rule 3

Rule 3 obliges a health agency collecting health information directly from an individual to inform that individual of:[47]

> *(a) the fact that the information is being collected;*
> *(b) the purpose for which the information is being collected;*
> *(c) the intended recipients of the information;*
> *(d) the name and address of:*
> *(i) the health agency that is collecting the information; and*
> *(ii) the agency that will hold the information;*
> *(e) whether or not the supply of the information is voluntary or*

[47] Health Information Privacy Code 1994, Rule 3(1)

mandatory and if mandatory the particular law under which it is required;

(f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and

(g) the rights of access to, and correction of, health information provided by rules 6 and 7.

The scope of the exceptions to rules 2 and 3 is narrower in the HIPC than in the equivalent part of the Privacy Act. This would usually indicate a stronger emphasis on transparency. However, as the NHI number is not normally collected directly from the individual its use is therefore only tangentially regulated by rule 3. This presents problems, even though it may not raise any legal issues.

Because the NHI is not normally collected directly from the individual concerned, there is no legal obligation for agencies to ensure that patients are aware of what the NHI is and is intended to accomplish.

There is also an issue with 'collection' vs 'assign'. Which is the most appropriate verb to consider in discussing the NHI? 'Assign', in this context, means to use the NHI number as a unique identifier of a particular person. 'Collect' means to obtain (other than by unsolicited receipt) personal health information about a person. Information which is collected is subject to various controls and, more importantly, has a purpose assigned to it by virtue of rule 1.

Rule 12, which deals with assignment, addresses one specific aspect of the NHI number, its status as a unique identifier. 'Collection' does not really address what is normally *done* with the NHI.

Transparency goes hand-in-hand with understanding. The HIPC as it stands does a little to require or encourage agencies to be open about their practices, but a generalised statement of purpose can, in practice, act as carte blanche to share information widely. For instance, a (hypothetical) statement on a hospital admission form that 'health information may be shared with other agencies involved in the provision of health services to you' would probably be sufficient to satisfy the obligations of rule 3 with regard to passing an individual's hospital file to specialists, PHOs, other DHBs and funders.

One possible way to remedy this, assuming it is seen as a problem, might be amending the HIPC to require transparency when assigning a unique identifier. This would be a significant departure from the general scheme of the Privacy Act and might be out of the scope of the

Privacy Commissioner's powers under section 46 of the Privacy Act 1993.

An alternative would be improving public awareness and understanding of the NHI by further education campaigns. As an example of what can be done, the NHI Upgrade Programme Consumer Advisory Group provided advice to the NHI Upgrade Programme Steering Committee regarding a pamphlet about the NHI number setting out some basic details of the NHI which could serve as a model for any further efforts in this direction. Following this recommendation a pamphlet and poster were designed and dispatched in 2005 for use by DHBs, GPs rooms and other health and disability service providers. Extensive information is also available on the NZHIS website.[48]

Rule 4

Rule 4 relates to the method of collection. While there are definite issues around transparency with the NHI, it would be a stretch to say these amount to 'unfair, unlawful or unreasonably intrusive' methods of collection. While, there are some questions about the collection of information from patients by enrolment into PHOs, these circumstances would normally involve the direct collection of information, and thus bring the transparency provisions of rule 3 into play. A transparent collection of an NHI number, or of information to be stored on the NHI, would probably not raise issues under rule 4.

Rule 5

Rule 5 regulates security, requiring health agencies to take reasonable steps to ensure that health information is held secure against loss and unauthorised access, use, modification or disclosure.

Security of the NHI is an important issue, and one that has been highlighted in all the health sector reviews to date. Security concerns in relation to health records and unique identifiers apply to both paper and electronic records, but it is the EHR that raises most public concern. While this may owe something to lack of understanding,

[48] See for example http://www.nzhis.govt.nz/nhi/index.html

there are legitimate concerns.

A small study carried out in 2004[49] indicated that the security of an EHR database was the main barrier preventing public acceptance.[50]

> *With centralised and distributed databases and linkages between various electronic systems, the chances of accessing large volumes of patient information as an unauthorised person increases significantly.*

Specific concerns that have been identified are[51]:

- Confidence in the privacy and security of creation and sharing of records
- The security aspects with regard to control of data and
- The risks that individuals who use the record may face, for example, not fully understanding what the record means and, thus, making incorrect conclusions.

The NHI is national, contains identifying information and is linked to sensitive health information. However, it also needs to be readily accessible if it is to fulfill its function. Initially this accessibility requirement was addressed by mailing out CDROMs with copies of the NHI information and providing health agencies with tranches of NHIs to assign. The limitations of this approach were identified in the Stevens report.[52]

Accordingly, careful consideration of the security obligations imposed by rule 5 is paramount. An appropriate set of security features around an EHR are authentication, access control, accountability, authorisation and availability.

Happily this has been a central focus, as evidenced by encryption and work on secure networks. [53] However, this is an area that will require ongoing attention, particularly as more initiatives like PrISM come

---

[49] Chhanabhai, Holt and Hunter, *Consumers, Security and Electronic Health Records*, 2006, page 5
[50] Above note 46, page 6
[51] Ryan, Boustead, *Universal electronic health records: A qualitative study of lay perspectives,* New Zealand Family Physician 2004, 31(3), pages 149-154
[52] Above note 16, appendix
[53] See for example MacRae, *NHI Encryption Methods*, 2006, available at http://hcro.enigma.co.nz/website/index.cfm?fuseaction=articledisplay&FeatureID=030606

online.

Rules 6 & 7

Access and correction do not appear to have raised major issues. Access requests involving the NHI itself would normally be made to the NZHIS, as the custodian of the Index. A search of complaint files revealed only two complaints that even mentioned NZHIS, both more than five years old. This may owe something to a lack of consumer knowledge about the NHI, but anecdotal evidence suggests NZHIS deals appropriately with access requests from consumers, when it receives them. It has a policy on its website at http://www.nzhis.govt.nz/access/access-appendix1.html.

Other NZHIS policies on access relate more to disclosure of information to researchers, DHBs and other government agencies.[54]

Rule 8

Criticisms of the NHI in the past have often focused on its perceived inaccuracy, and accuracy was a major problem with the NHI's predecessor, the NMPI. A commonly cited problem is the existence of many millions more non-deceased, non-duplicate unique records than New Zealand has citizens.

As a national database, relying on collection of information by third parties with no personal stake in the accuracy of the information collected, there are obvious accuracy challenges. The flaws inherent in early attempts to address these challenges were identified in Stevens' report, particularly practices such as sending out CD-ROMs containing the NHI in loosely encrypted text form.

An upgrade programme which has been ongoing since 2003 has removed many of the duplicates.[55]

[54] Available at http://www.nzhis.govt.nz/access/index.html
[55] Available at http://www.nzhis.govt.nz/nhi/nhifaq.html

Rule 9

The purpose of rule 9 is to prevent health information being retained perpetually as a matter of course. It does this by requiring health agencies to dispose of health information when they no longer have a lawful purpose for holding it.

NHIs are never reallocated – once the consumer with whom a particular NHI number is allocated dies, the fact and date of death are added to the register. Accordingly, the NHI is effectively a perpetual data store.

Rules 10 & 11

As the NHI is personal health information, rules 10 and 11 apply to its use and disclosure. In general, health information may be used or disclosed where that use or disclosure is for the same purpose for which the information was obtained. NHI-related information is normally obtained to provide health services to the individual concerned or for broader research and population health purposes. [56]

Problems may arise because the HIPC does not tightly regulate the use of the NHI. Accordingly there is a risk that a use or disclosure which is acceptable in terms of the HIPC may be viewed as being privacy neutral when in fact it is not. One suggestion has been for a voluntary code of conduct to be issued and promulgated around the use of the NHI by the Ministry of Health.

Rule 12

Unless restrictions are placed on who may assign a unique identifier, there is a risk that it may become a de facto national identifier across many sectors. Widespread access to unique identifiers, even without a name attached, may offer little or no privacy if many people are easily able to link a number to an identity.

Principle 12 of the Privacy Act was devised in response to this risk.

---

[56] See for example http://www.nzhis.govt.nz/nhi/nhifaq.html#02i

The underlying purposes of principle 12 were summarised by the Privacy Commissioner in *Necessary and Desirable.*[57]

> *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.*
>
> *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.*

The NHI, as a health unique identifier, is subject to rule 12 of the Health Information Privacy Code 1994. Rule 12 significantly modifies principle 12 with respect to the NHI, effectively creating a wide but regulated discretion for specified health agencies to assign a unique identifier that has already been assigned by another agency.

Rule 12 reads:

> **UNIQUE IDENTIFIERS**
>
> *(1) A health agency must not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the health agency to carry out any one or more of its functions efficiently.*
>
> *(2) A health agency must not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless:*
>
> *(a) those 2 agencies are associated persons within the meaning of section OD7 of the Income Tax Act 1994; or*
>
> *(b) it is permitted by subrule (3) or (4).*
>
> *(3) The following agencies may assign the same National Health Index number to an individual:*

---

[57] Office of the Privacy Commissioner, Necessary and Desirable, 1998, 2.14.5. The summary outlined above was itself a summary of Dr Paul Roth, writing in *Privacy Law and Practice*.

(a) any agency authorised expressly by statute or regulation;
(b) any agency or class of agencies listed in Schedule 2.

(4) 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.

(5) A health agency that assigns unique identifiers to individuals must take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

(6) A health 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 or for a purpose that is directly related to one of those purposes.

(7) Subrules (1) to (5) do not apply in relation to the assignment of unique identifiers before the commencement of this code.

(8) Subrule (6) applies to any unique identifier, whether assigned before or after the commencement of this code.

The main differences between rule 12 and principle 12 are found in rule 12(3) and 12(4). Rule 12(3) provides an effective exemption, for agencies listed in Schedule 2, to the prohibition on assigning a unique identifier that has already been assigned. Rule 12(4) allows for the assignment of health practitioner unique identifiers on application to the Privacy Commissioner and does not raise NHI issues.

Rule 12 modifies the principle 12 prohibition on the assignment of NHI numbers by different agencies. As the only part of the code, apart from its ancillary Schedules, specifically dealing with unique identifiers it is naturally the initial focus. However, rule 12 only deals with those aspects of the NHI particular to its identity as a unique identifier.

Rule 12 also restricts the NHI by listing, in Schedule 2, a set of agencies, or classes of agencies, that are permitted to assign it. The Privacy Commissioner proposes to broaden the scope of Schedule 2, in order to facilitate the development of national EHR systems. Agencies and practitioners wishing to gain online access to the NHI must sign

the *Deed of Agreement for Access to National Health Index and Medical Warnings System*. The Agreement provides privacy protective obligations such as, in summary, that:

> *The user must ensure that all information obtained from the NHI and MWS is used and disclosed solely for a purpose and in a manner permitted by law;*
>
> *The user must comply with all reasonable directions and instructions issued by the Ministry in regards to access to the NHI and the MWS;*
>
> *The user must put in place procedures and policies to ensure the user's employees, contractors and agents are informed of their security and confidentiality obligations under the HIPC and Privacy Act, and must:*
>
> > *(a) develop written policies and procedures to be followed by its employees, agents and contractors;*
> > *(b) establish controls, including:*
> >
> > > *(i) the use of passwords, credential tokens or other mechanisms; and*
> > > *(ii) user identification;*
>
> *The user must ensure that only authorised employees, contractors and agents of the user who have a legitimate need to access health information are permitted access to the NHI and MWS;*
>
> *The user must ensure the accuracy, integrity and completeness of information supplied to the NHI and MWS.*