

submission

Submission by Privacy NSW
to the Australian Health Ministers Advisory Council (AHMAC)
National Health Privacy Working Group

in relation to the

Draft National Health Privacy Code

Issue date: April 2003



privacynsw

To National Health Privacy Working Group of the Australian Health Ministers
Advisory Council c/- Australian Department of Health and Ageing, forwarded in
May 2003 in response to Draft Code and Consultation Paper released in
December 2002

This submission is not intended to represent the views of the NSW Government
or the Attorney General of NSW.

Scope of Submission

This submission has chosen to concentrate on select issues raised in the Discussion Paper as well as some issues relating to the drafting of the proposed Code (NHPC) and National Health Privacy Principles (NHPPs). One difficulty in addressing some of these issues is that whether a particular provision is adequate will often depend on the broader issues of scope and implementation.

I. Comments on Specific Issues raised in the Discussion Paper

➤ Implementing of the Code

3. *What are the main issues relating to implementation that should be considered by the Privacy Working Group?*
4. *Should the code be mandatory or voluntary? Why?*

While Privacy NSW is supportive of the development of a nationally consistent approach to health privacy regulation, we are nevertheless concerned about the standard of privacy protection that will be adopted.

The development of a Code establishing uniform standards can be seen as an appropriate and practical solution to some of the complexities and inconsistencies of current state and federal health privacy legislation. We would be inclined to support the NHPC if the standard of privacy protection is equivalent to or greater than that afforded by the *Health Records and Information Privacy Act 2002 (NSW)* (HRIPA). However we recognise that equivalence need not require identical forms of expression or identical ways of addressing specific issues. Thus, while Privacy NSW welcomes the release of the draft code, the Privacy Commissioner reserves his decision whether or not to endorse any final draft of the NHPC.

Ultimately, however, the status of the NHPC will be a matter for Federal, State and Territory health ministers. The effective implementation of the Code will require commitment and co-operation from all decision-makers in order to overcome the problems inherent in our federal system of government.

The issue of implementation is in part tied to the final scope and content of the NHPC. The *Consultation Paper* unfortunately provides no detail as to what form the NHPC would take if it were to be made a mandatory code. As such, we can only speculate over some features of the Code and the legal implications to which they would give rise. How would a mandatory NPHC operate along side existing state and federal privacy statutes? Would a mandatory code be enacted as legislation or adopted as a code within the existing framework of the Commonwealth *Privacy Act*? Could the Code have a more limited function of addressing privacy standards where information is exchanged between jurisdictions?

Clearly, the question of the status of the NHPC raises complex and difficult issues given the enactment of specific health privacy legislation by the governments of NSW, Victoria and the ACT. While a mandatory code would be relevant for those jurisdictions without specific health privacy regulation, it may not be workable for those States and Territories with their own health privacy laws.

On the other hand, a voluntary code presents numerous advantages over a mandatory code. Although such a code would lack enforcement mechanisms to secure compliance, a voluntary NHPC would be less complicated to integrate into the existing regulatory framework. Further, it would provide flexibility in terms of responding to the changing needs of the health care sector. A voluntary code would probably be reviewed, up-dated and fine-tuned on a timelier basis than a mandatory code.

Another option would be to allow the health ministers to determine the status of the NHPC as it applies to their state or territory. This would allow them to consider the needs of their own constituency and to assess how the NHPC would be best implemented in their particular jurisdiction.

➤ **Scope**

5. *Your views are sought on the advantages and disadvantages of the three approaches outlined above to assist the Privacy Working Group in reaching a decision that will provide both the most workable solution and the best level of privacy protection.*
6. *What would be the most reasonable and appropriate approach to take? Are there any other factors that should be considered?*
7. *Are there any other options that aren't considered in the discussion paper?*

The Discussion Paper suggests that the NHPC could either have a limited application to health service providers, apply to all health information (presumably within some broader limits), or apply principally to health service providers but also in some circumstances to other associated organisations, such as employers or insurers. In our view, Option 2 would be the most appropriate model with regards to the scope of coverage of the NHPC. We acknowledge that a non-health organisation may collect both health and other types of personal information and, hence, may be subjected to both health privacy regulation as well as general privacy legislation under the *Privacy Act 1988* (Cth). It may therefore be necessary to consider simplifying legal compliance with different privacy laws where overlaps occur.

An argument could be made that such organisations err on the side of caution and adopt the higher standard of privacy protection for all personal information they handle. In our increasingly integrated and networked environment, health information is collected, combined, exchanged and stored with non-health information with greater ease and efficiency. Possible non-consensual disclosure or misuse of personal health information has equally serious consequences for the individual concerned whether the relevant organisation is from the health care sector or another service industry. At the same time we recognise that the health sector is governed by professional standards and ethics for which there is no precise equivalent in other sectors.

The following discussion of the adequacy and appropriateness of the proposed NHPPs is largely dependant on how the issue of scope is resolved. Standards that may apply to clinical records will not necessarily carry over to the multiplicity of other functions which health information can serve.

The NHPPs

The discussion of the NHPPs invites a comparison with the National Privacy Principles in Schedule 3 of the Privacy Act 1988 (NPPs), the Health Information Privacy Principles in Schedule 1 of HRIPA (HPPs) and the Health Privacy Principles in Schedule 1 of the Health Records Act 2001 (Vic) (HPPVic). In seeking to reconcile these different standards the NHPPs can be seen to reduce the overall degree of privacy protection in some significant respects.

➤ **NHPP 2 Use and Disclosure**

➤ *Disclosure for secondary purposes*

Principle 2.2(a)(ii) draws on an exemption which is variously expressed in NPP 2.1(a)(ii), HPP 11(1)(b) and HPPVic 2.2(a) whereby information can be used or disclosed for a directly related secondary purpose if an individual would reasonably expect an organisation to use or disclose it for that purpose.

In effect this exemption permits an agency to substitute its own views, on the reasonableness or otherwise of the individual's expectations as to how their health information could be used, for the views held by individuals themselves. The systematic application of such a test in a Code specifically designed to reflect best privacy practice in relation to health records represents a serious diminution of the level of protection appropriate to health information. It is inconsistent with international standards for the protection of health information (see for example Article 8.3 of the European Union's *Data Protection Directive*), and with accepted legal and professional standards of medical confidentiality, both of which require express consent to disclosure except in much more narrowly defined circumstances.

The test is also inconsistent with a main aim of information privacy legislation, to give individuals a degree of control over how their information is used. Instead it makes the agency the arbiter of the extent of its obligations to individuals by substituting a standard of reasonableness for the wishes of the individual. Recent surveys of individuals' attitudes to the privacy of their personal information show that people have a significant range of different views as to when disclosure is appropriate.¹ A reasonableness standard is therefore difficult to apply in a fashion which empirically reflects the nature of people's concerns.

For all of these reasons I consider that the appropriate test in relation to use of health information for a directly related purpose should be one which requires express consent, or at the minimum a provision similar to section 18(1)(a) of the NSW PPIP Act which is conditional on the agency having no reason to believe the individual would be likely to object.

➤ *Teaching Health Students*

19. *Should students in the health professions be subject to the Code to the extent that they handle health information? If not, why not?*
20. *Under what circumstances, if any, should patient or client consent be sought for the use or disclosure of health information for the purpose of training students in the health professions?*
21. *Is it appropriate for "training" of students in the health professions to be deemed to be a directly related secondary purpose under the Code or is it adequate to rely on NHPP 2.2(f) for this activity? If so, how should "training" be defined?*

We believe that it is necessary to regulate the use of health information for training purposes as part of the process of balancing the privacy of health clients with other interests. It is not appropriate simply to assume or imply consent by virtue of the fact that a service is provided in a teaching hospital or with the assistance of trainees. Having said this we recognise the need for special provisions to facilitate the use and disclosure of health information by

¹ Roy Morgan Research for Office of the Federal Privacy Commissioner, *Privacy and the Community, July 2001 paragraphs 4.8-4.10, 4.16, 4.24-4.27.* [Community, July 2001 paragraphs 4.8-4.10, 4.16, 4.24-4.27.](#)

trainees in the health sector. This may involve identifying and addressing different issues for employee training and student placements.

In New South Wales, training is identified as a secondary purpose under HRIPA, HPP 10 (e) & HPP 11(e). To provide clarity and guidance, our Office has commenced a consultation process to develop specific guidelines for the use and disclosure of health information for professional training purposes under HRIPA.

➤ *Law enforcement*

NHPP 2.2(i) and (j) would create exemptions that are not entirely consistent with each other. NHPP 2.2(j) would create a lower standard for disclosure to law enforcement agencies than currently exist under NPP 2 of the *Privacy Act* or HPP 11(1)(j) of HRIPA, which require the investigation of an offence or serious misconduct or a belief that an offence has been committed. Even with the qualification that *use or disclosure would not be a breach of confidence*, which implicitly recognises that some forms of information may require that there be express legal authority to justify a disclosure, this represents an inadequate level of accountability for such disclosures. In any case it's unlikely that those responsible for making disclosures would be aware of all the implications of the reference to the legal obligation of confidentiality.

➤ *Where an individual is incapable of providing consent*

We are not convinced that NHPP 2.4 adequately addresses all of the issues which are likely to arise in relation to people with diminished capacity. A substitute consent model may be appropriate in relation to some clinical situations but is not likely to adequately address all the contexts where it is proposed to use or disclose health information and consent is not easily obtained. It too easily suggests that the views of people with a diminished capacity for consent should not be taken into account.

For the information of the Working Group, Privacy NSW is in the process of developing guidelines to assist agencies with their privacy obligations where the

individual concerned lacks capacity to provide consent. These guidelines deal with incompetent adults and minors separately. They are referred to as the *Guidelines on Consent and Capacity Under the PPIP Act and Children and Young People and Privacy*. For more information see:

< <http://www.lawlink.nsw.gov.au/pc.nsf/pages/guidelines>>.

➤ **NHPP 4 Data security and data retention**

35. *Do the requirements in National Health Privacy Principle 4 reflect appropriate requirements for the retention of records? Are there any further issues that should be addressed?*

36. *A number of timeframes are set as to when information may be destroyed. Are these appropriate?*

The development of electronic health records (EHR) will enhance and expand the scope of both primary and secondary uses of health records including care, legal, research and educational activities. EHR will make it increasingly easier to store, access and disseminate personal health information. However, the application of such technology may not yet be sufficiently sophisticated to meet the needs of health care administration while at the same time adequately protecting patient data. The mere fact of ready availability increases the pressures on health custodians to allow secondary use of health information. Examples of information security breaches illustrate that, like other technologies, health information security systems are also susceptible to technological or human errors.²

Given the risks of retaining health records, in either hard copy or electronic format, Privacy NSW would be disinclined to support an extension of current statutory retention periods in the absence of substantive justifications and adequate security guarantees.

There are also challenges presented by the processing of genetic information. Recent advances in genetic research and therapy give rise to new concerns

² See Carter M, "Patient privacy in the electronic era: legal and privacy considerations" (2000) 8(9) *Australian Health Law Bulletin* 117 at 117.

over the maintenance, security and retention of health records.³ Should clinical genetic records be held separately from general health records? Are existing security measures adequate given the sensitive nature of genetics information? And should records be retained indefinitely on the grounds that they could be of benefit to future generations?

It may be necessary in some circumstances to separate genetic records regarding familial conditions from general health records. Genetic records tend to represent families and not just the individual and therefore it may not be appropriate for them to be kept with general health records.

It may also be necessary to clarify the retention time frame for different kinds of health information in order to avoid the situation where health organisations may feel compelled to hold onto health records for longer than any prescribed retention period.

37. *Are there any circumstances when an individual should be able to request deletion (as distinct from correction and masking) of health information from his/her record?*

We are aware of the argument that is sometimes advanced that the importance of maintaining accurate records of professional conduct and treatment preclude the deletion of health records. The recent NSW Court of Appeal case of *Crewdson v Central Sydney AHS* [2002] NSWCA 345, can be seen to reinforce a line of decisions under the NSW *Freedom of Information Act* which lend support to this position.

Assuming a relatively broad scope for the definition of health information we do not see that this approach is consistent with striking an appropriate balance between privacy and the development of electronic health records. It overlooks the widely expressed concerns people have about the potential misuse of their health information and the greater risks of misuse where such information can

³ Meschino W S, "Results of a national survey re: retention and maintenance of clinical genetics records" (2001) 69(4) *American Journal of Human Genetics* 443.

be readily retrieved. It also ignores the wide range of different purposes for which health information is retained.

There is already some recognition of the need for limits on retention of health records. For example Chapter 8 of the National Health and Medical Research Council's 2000 *Guidelines for Genetic Registers and Associated Genetic Material* clearly recognises the need to dispose or return genetic sample and information in appropriate circumstances. In the NSW HRIPA, HPP 8 recognises the privacy interest in limited retention by specifically providing for amendment of inaccurate, irrelevant out of date or misleading health information by way of deletion.

➤ **NHPP 5 Openness**

38. *Are there any issues with the requirement for an organisation to be open about its information management policies as expressed in this Principle?*
39. *Should the aim of NHPP 5.2 be to provide information when requested to a specific individual whose information is held with the organisation, or should it aim to make general information available to anyone?*
40. *Is it appropriate for public and/or private sector organisations to be required to maintain and publish a health information Digest akin to the Commonwealth's Personal Information Digest? If so, why?*

We recognise that the openness principle is susceptible of different interpretations in different contexts and that its application to health information may differ from its application to public sector records more generally. An expansive approach to the openness principle is relevant to the functions and operations of public sector agencies and consistent with the notion of open government. For the health sector openness should reflect the more personal relationship between provider and client. For example, the Personal Information Digest may assist in the understanding of how personal information is handled by public sector agencies, but would be a cumbersome process to adopt in the health care sector given the greater variation in the size and functions of its constituent units.

For these reasons, Privacy NSW favours the more responsive approach that the Discussion Paper describes as the Victorian model; see also HRIPA, HPP 6.

➤ **Complaints mechanisms**

70. *Should complaints related to possible breaches of the National Health Privacy Code be handled by a single body in each State or Territory?*

71. *What other issues relating to complaints would you like to see considered by Privacy Working Group?*

Under NSW health privacy legislation, Privacy NSW is the designated body to receive, investigate and conciliate complaints regarding possible breaches of the Health Privacy Principles. However, our organisation is also able to refer complaints which we consider are more appropriately dealt with by other organisations, for instance, the Health Care Complaints Commission and the Office of the Federal Privacy Commissioner (HRIPA sections 65 & 66). People who are aggrieved by conduct in breach of the HPPs by NSW public sector agencies can seek review under Part 5 of the PPIP Act. Part 5 Review does not apply to non-government holders of health information.

We recognise that the degree of overlap between State and Federal privacy legislation, and other forms of regulation affecting health providers, may confuse health consumers. However we believe that the ability to co-operate and refer matters to other bodies provides a workable mechanism to determine which is the most appropriate body to respond to a particular complaint.

To the extent that the NHPC aims to enforce nationally consistent standards it will be important to ensure that people's ability to seek remedies are not frustrated by uncertainties about which is the appropriate jurisdiction. The code development process could make a useful contribution to extend the process of referrals between jurisdictions. The extent to which organisations should seek to remedy grievances internally also needs to be considered. This should not be done in a way that discourages complainants from seeking assistance from an appropriate regulator or drawing their attention to a problem. The systemic

nature of many privacy breaches makes it desirable that they are not resolved on an ad hoc basis.

➤ **Selling of health data**

78. *As non-identifiable data cannot identify individuals, should individuals be able to determine the use to which that data is put?*

79. *Should the law prevent or regulate the selling of this data? If so, when? Consider the impact on the following scenarios:*

- *the purchase of comprehensive data for private commercial purposes; and*
- *Official Government and research publications that are sold, but which are generally available to the community, and are published to provide demographic information relevant to public health and educational activities.*

80. *Are any additional laws necessary to regulate the sale of non-identifiable data?*

The fact that current privacy legislation is restricted to identifiable personal information does not mean that no privacy issues arise in relation to non-identifiable health information. As information such as health records becomes a key asset in our “information society” we can discern increasing pressures for the commodification of personal data.

Public attitudes regarding the use of non-identified information should be a primary consideration in evaluating the proposal for the commercialisation of health data. A survey commissioned by the Office of the Federal Privacy Commissioner suggests that the current practice of using non-identified information for health research may not be consistent with prevailing public expectations. The survey concluded that more than half of the population (61%) were of the view that consent should be sought before unidentified information could be used for medical research.⁴ The response is likely to be higher where views are sought on the sale of health data for private commercial purposes.

⁴ OPFC, *Privacy and the Community*, July 2001, prepared by Roy Morgan Research, at 37.

Intensive use of non-identified health data may also have broader social implications. Aggregated personal information is still capable of adversely affecting people, for example if it serves as a basis for discriminating against specific ethnic or geographically located groups.⁵ The Australian Consumers Association has voiced concerns that the existing high level of private marketing expenditures by pharmaceutical corporations can influence health priorities. A recent article in their journal noted that the large global pharmaceutical companies spend twice as much on marketing and administration as they do on research and development.⁶

Furthermore, academic commentators have queried the extent to which information can be permanently anonymised. A study by Dreiseitl et al suggest that although the “recent advances in anonymization algorithms provide increased levels of protection, it is still possible to calculate approximations to the original data set [and] in some cases, one can even uniquely reconstruct entries in a table before anonymization.”⁷ In the same vein, Sweeney has illustrated the possibility of linking de-identified information with accessible data held in public registers.⁸ Privacy NSW therefore urges the Privacy Working Group to critically analyse both the statistical techniques applied to de-identified health information as well as the possibilities for reversing such processes.

The necessary regulatory responses to the sale of health information may vary depending on the nature of the intended use of personal data. Under existing privacy legislation patient rights to privacy may be outweighed by a legitimate public interest such as access to medical records for research purposes. The requirement for approval of research projects by Human Research Ethics Committees has proven to be a reasonably effective safeguard against possible

⁵ For a recent Canadian summary of some of the literature on discriminatory use of health information see [Pchapter Poudrier J, “ “Racial” categories and health risks: epidemiological surveillance among Canadian First Nations” in](#) Lyon D ed, *Surveillance and Social Sorting*, (New York & London: [Routledge](#), 2003) [at 111-134](#).

⁶ Ballenden N & Goddard M, “The Hard Sell” (Summer 2003) No 94 *Consuming Interest* 6, at 6.

⁷ Dreiseitl S, et al, “Disambiguation data: Extracting information from anonymized sources” (2002) 9(6) *Journal of the American Medical Informatics* S110, at S110.

⁸ Sweeney L, “Guaranteeing anonymity when sharing medical data, the Datafly system” (1997) *Journal of the American Medical Informatics Association* 51.

inappropriate or unethical use of health information. In contrast, the on-sale of health data without restrictions on its subsequent use is less obviously and less directly in the public interest.

It could be argued that the sale of non-identified information should be permitted where it does not present a threat to patient health or privacy. However, the benefits of such an exchange may essentially be confined to the two parties involved, to the detriment of any broader public interest or groups with which subjects can be identified. An earlier private sector initiative has illustrated that even if private corporations were not provided with direct access to identifying information, their proposed marketing strategies may prioritise corporate interests and place patient welfare at risk.⁹

Given such concerns, Privacy NSW would urge the Working Group to adopt a more critical approach to the proposed sale of patient health data albeit where this data is non-identifiable. In addition to the concerns raised above, other issues of concern include:

- what is the specific nature of non-identified information sought and how is this information intended to be used;
- to what extent should patients bear the risk of re-identification; and
- what should be appropriate requirements for the disclosure and reporting of the financial benefits acquired by both parties from the on-sale of data, if any?

II. Further Comments on the Content of the Draft NHPC

➤ Part 2 Application of the Code

Paragraph 2 excludes the activities of holders of quasi-judicial offices in relation to the exercise of their quasi-judicial functions. The scope of this definition involves a disturbing lack of precision and has the potential to create a very broad exemption for which there is no clear justification.

Page 45 of the *Consultation Paper* implies that this is intended to apply to a small number of agencies which perform court like functions and which will be covered by the rules applying to these bodies. With respect this argument is not persuasive. There are significant distinctions to be made between the treatment of information in courts, formal tribunals and other bodies that make formal determinations. Any public sector agency that makes formal determinations in relation to an entitlement or benefit could be seen to be exercising a quasi-judicial function. Current difficulties experienced by privacy practitioners in determining the proper scope of exemptions for the exercise of judicial functions will no doubt be magnified with the introduction of a much wider degree of uncertainty in relation to quasi-judicial functions.

We recommend that the exemption be brought back to courts and tribunals exercising judicial functions and that these functions be defined in terms similar to section 6(3) of the NSW *Privacy and Personal Information Protection Act* or section 13 of HRIPA.

Paragraph 3(1) gives a general exclusion for health information contained in a document that is a generally available publication unless it has been obtained in contravention of this Code, or which is held in a library, museum, archive or similar public repository. Paragraph 3(2) refers even more loosely to health information *that is generally available to members of the public* in a manner which is inconsistent with the more restrictive categories referred to in paragraph 3(1). The breadth of this latter exemption involves a misunderstanding of the proper function of information privacy regulation. It assumes that information that has found its way into the public domain is not generally worthy of protection unless it is known to have been improperly obtained or disseminated. This assumption is not justified. Just because information is obtained from a publicly available source does not mean that its subsequent collection and use is not capable of harming individuals. The proposed safeguard excluding information that has been obtained in

⁹ Robotham J, "Doctors worried about Ethics of Patient Database", *Sydney Morning Herald*, 30 December 2000, at 2; see also Beck, M "Working for Them", *Surveillance &*

contravention of the Code is impracticable as a basis for including or excluding specific kinds of information. It allows people and organisations to further violate the privacy of individuals once their information has been improperly disclosed. Our recent experience of media comment based on disclosures of the health information of correctional inmates by NSW public sector agencies and Ministers illustrates this process.

➤ **Part 4 Interpretation**

The definition of authorised representative, derived from section 85(6) of the Victorian Health Records Act, is a useful addition to mainstream privacy regulatory practice where the issue of substitute consent is often imprecisely addressed.

The references to prescribing health services and health service providers as exempt is taken from the Victorian *Health Records Act*. While the definition of health service provider in section 4 of HRIPA and the regulation making power in section 75 permit the proclamation of exempt health service providers there must be some doubt as to whether it is appropriate to import these definitions into a code which aims to enforce national standards so that any participating jurisdiction can opt out simply by exempting a particular class of service or provider. For example one could imagine some Governments exempting health services provided in a correctional context, in a way that significantly compromised the secure transfer of such information between jurisdictions.

The definition of law enforcement agency to include agencies responsible for the performance of functions or activities directed towards administration, prevention, detection, investigation or remedying of breaches of the law that impose penalties or sanctions for a breach, and the equally broad definitions of law enforcement functions seem to include a much broader range of Commonwealth, State and Territory agencies and activities than would normally be recognised as law enforcement related. The impact of these definitions is

ostensibly qualified by the reference to the general law on confidentiality (note 6 on page 19).