



Australian Government

Office of the Privacy Commissioner

**National Registration and
Accreditation Scheme for the
Health Professions (NRAS):
Proposed arrangements for
information sharing and privacy**

**Submission to the
Australian Health Ministers'
Advisory Council**

December 2008

Table of Contents

Executive Summary	2
Office of the Privacy Commissioner	3
Background	3
Part 1: Addressing information-handling through a comprehensive privacy framework	4
Key issues for privacy and information handling under the NRAS	5
Implementing an appropriate privacy regime	5
Privacy impact assessments.....	6
Handling of sensitive information	7
Secondary uses of practitioners' information	8
Deidentifying workforce and statistical information	9
Protection of unique identifiers.....	9
Assessing risks and security measures for amalgamated databases	10
Part 2: Comments on specific proposals in the Consultation Paper	11
Information to be collected under the scheme	11
Information to be collected for initial registration purposes	11
Employer details	12
The unique identifier	12
Identity checking on initial registration	13
Information to be collected for workforce planning purposes.....	14
Public availability of de-identified workforce planning statistics.....	14
Publicly available information	15
Information on the public register.....	15
De-registered practitioners.....	16
Recording of conditions on practice	16
Release of public register information	17
Public access to the findings of formal proceedings.....	18
The privacy regime	19
Legislative options	19
Information sharing	20
Enabling e-health developments	20
Research	20
Professional Services Review Scheme (PSR Scheme)	21
Medicare Australia.....	22
Overseas trained practitioners	22
State and Territory government health bodies	23
Notification to Commonwealth, State and Territory health departments.....	24
Law enforcement agencies.....	24
Trans-Tasman Mutual Recognition	25
Overseas regulatory authorities.....	25
Health records.....	26
Transitional issues – Supply of information from existing boards to the agency (Consultation Paper part 9.1)	26
Conclusion	27

Executive Summary

1. The Office of the Privacy Commissioner ('the Office') supports the development of a National Registration and Accreditation Scheme for the health professions ('NRAS') that protects and respects practitioners' privacy through sound information-handling practices, while maintaining high quality and safety standards throughout the health sector.
2. The Office is confident that both these outcomes can be achieved through the ongoing consideration of privacy issues during the scheme's development. The Office welcomes the release of a public consultation paper dedicated to privacy and information sharing. As explored in this submission, the consultation paper identifies a range of information-handling matters that will be important in ensuring that appropriate information flows can occur, and that adequate privacy protections apply.
3. There are two main parts to this submission. Part 1 outlines a number of particular issues which, in the Office's view, are central to ensuring privacy-friendly design and sound information-handling practices for the NRAS system. These matters include:
 - implementing an appropriate privacy regime
 - privacy impact assessments
 - handling of sensitive information
 - secondary uses of practitioners' information
 - deidentifying workforce and statistical information
 - protection of unique identifiers, and
 - assessing risks and security measures for amalgamated databases.
4. The submission suggests that these and other issues be addressed through the adoption of a comprehensive privacy framework, involving a combination of Design, Technology, Legislation and Oversight measures.
5. Part 2 of this submission responds to each of the specific proposals for information sharing and privacy outlined in the consultation paper. The Office is generally supportive of these proposals, subject to further considerations of detail which, the Office suggests, would be best addressed through a formal privacy impact assessment process. In particular, the Office supports the adoption of a privacy regime based on existing standards under the *Privacy Act 1988* (Cth), rather than a separate set of principles or other laws.
6. Overall, the Office welcomes the attention to privacy issues under the NRAS. With consistent attention to these issues, including through a comprehensive privacy impact assessment, the public safety objectives of the scheme can be achieved in a way that respects and protects the privacy of our health practitioners.
7. The Office looks forward to further opportunities for public consultation, including exposure drafts of future legislation, and will work to provide further privacy advice on the NRAS as it is developed and implemented.

Office of the Privacy Commissioner

1. The Office of the Privacy Commissioner ('the Office') is an independent statutory body responsible for promoting an Australian culture that respects privacy. The Office, established under the *Privacy Act 1988* (Cth) ('the Privacy Act'), has responsibilities for the protection of individuals' personal information that is handled by Australian and ACT government agencies, and personal information held by all large private sector organisations, health service providers and some small businesses. The Office also has responsibilities under the Privacy Act in relation to credit worthiness information held by credit reporting agencies and credit providers, and personal tax file numbers used by individuals and organisations.

Background

2. The Office welcomes the public submission process for the National Registration and Accreditation Scheme for the Health Professions ('NRAS' or 'the scheme'). The Consultation Paper on *Proposed arrangements for information sharing and privacy* ('Consultation Paper'¹) presents an opportunity to incorporate sound information-handling practices into the development and implementation of the NRAS, and to minimise privacy risks for those involved.
3. The Consultation Paper is one of several for the scheme. This paper is of particular relevance to the Privacy Commissioner's role and responsibilities for promoting and protecting privacy in Australia.
4. The Intergovernmental Agreement (IGA) for the NRAS describes the scheme's main objective as: 'To establish a single national registration and accreditation scheme for health professionals'.² Further objectives are:
 - to provide for the protection of the public through proper registration processes
 - facilitate workforce mobility in Australia and reduce 'red tape' for practitioners
 - facilitate high quality education and training for overseas-trained practitioners
 - have regard to the public interest in access to health services, and
 - enable the development of a flexible, sustainable and innovative Australian health workforce.³

¹ Available at www.nhwt.gov.au/natreg.asp. Direct link (as at 12/12/08): www.nhwt.gov.au/documents/National%20Registration%20and%20Accreditation/Consultation%20Paper%20Info%20Sharing%20and%20Privacy%202.0.pdf.

² Intergovernmental Agreement for a National Registration and Accreditation Scheme for the Health Professions ('the IGA'), 'Objectives', para 5.1 (available at www.nhwt.gov.au/natreg.asp). The ten professions currently registered are physiotherapy, optometry, nursing and midwifery, chiropractic care, pharmacy, dental care (dentists, dental hygienists, dental prosthetists and dental therapists), medicine, psychology and osteopathy.

5. The Office acknowledges the importance of these objectives, and agrees with the range of factors to be addressed in the scheme's information sharing and privacy arrangements, as outlined in the Consultation Paper. These include:
 - the need for public safety and quality healthcare
 - government transparency and accountability
 - balancing the rights and interests of consumers and health practitioners
 - facilitating the flow of necessary information to allow registration/accreditation boards and the national 'agency' to fulfil their functions, and
 - clarifying what privacy protections apply under the scheme.⁴
6. The Consultation Paper refers to multiple occasions for public input on the NRAS, including an exposure draft of legislation to be released for comment once proposals and policies are finalised (page 4). In November 2008, the Privacy Commissioner was briefed on the privacy aspects of the scheme, and the Office's representatives also attended a public forum on the Consultation Paper in Melbourne. The Office supports ongoing opportunities for public consultation as the scheme develops.

Part 1: Addressing information-handling through a comprehensive privacy framework

7. With information-handling it is critical that privacy protections are examined and built in from the beginning of a project's development. The handling of personal information also needs to align with both individual and public expectations. Public consultation, privacy impact assessments (PIAs) and the ongoing involvement of the Privacy Commissioner (and other relevant privacy and information commissioners) can all assist in this process.
8. A useful way of building a comprehensive privacy framework into any large-scale project involving personal information-handling is to address four key aspects:

Design + Technology + Legislation + Oversight (DTLO).

Addressing each of these factors will help to ensure a well-balanced foundation for the scheme.

9. Such a foundation would ensure that the NRAS:
 - protects the public interest in safe and high quality healthcare, fostered by appropriate information flows; and

³ IGA, para 5.3.

⁴ *National Registration and Accreditation Scheme for the Health Professions (NRAS) Consultation Paper – Proposed arrangements for information sharing and privacy* ('Consultation Paper'), pp 5-6.

- respects and protects the privacy interests of health professionals and other individuals involved.

Positively, the Consultation Paper identifies these priorities as the ‘two key functions’ of the scheme’s regulatory framework on information sharing and privacy (p 6).

10. In practical terms, respecting and protecting privacy includes giving people the ability to exercise sufficient control and choice over the way their personal information is handled, and safeguarding that information from misuse or unexpected treatment. More broadly, privacy interests can also mean retaining reasonable autonomy to go about our lives (such as working in a chosen profession) without undue interference, and to be treated as a valued member of society.
11. The Office’s *Community Attitudes Survey 2007* revealed a very high level of trust in health service providers – more than any other sector.⁵ The NRAS will provide an opportunity to reinforce that trust by maintaining professional standards. At the same time, by ensuring that the scheme employs good information-handling practices, the NRAS will acknowledge the important place of health service providers in the Australian community. This aligns with the scheme’s objective of a sustainable Australian health workforce, and the need for transparent and accountable governance (see paragraphs 4 and 5 above).

Key issues for privacy and information-handling under the NRAS

12. There are a number of key considerations for privacy and information sharing under the NRAS which are outlined below. The specific proposals outlined in the Consultation Paper are addressed in Part 2 of this submission.

Implementing an appropriate privacy regime

13. The framework of privacy regulation and governance arrangements for the NRAS is a fundamental consideration. Decisions on this matter will determine what standards of privacy and information-handling will be required under the scheme, how privacy issues will be regulated and by whom.
14. Generally, the activities of Australian Government agencies and large private sector organisations are regulated by the federal Privacy Act. Nevertheless, due to the nature of the NRAS as an intergovernmental project, the Office agrees that ‘The national scheme legislation will therefore need to be clear about what information sharing and privacy regime will apply to the scheme.’⁶

⁵ 91% of respondents said they trusted the health sector when it came to handling their personal information – more than any other sector. See the Office of the Privacy Commissioner, *Community Attitudes to Privacy 2007*, p 17, available at www.privacy.gov.au/publications/rcommunity07.pdf.

⁶ Consultation Paper, p 6.

15. As the Consultation Paper points out, there are different laws which regulate privacy at the federal and (some) State and Territory levels. The jurisdictions of these laws may sometimes appear to overlap, such as in the private health sector. While the principles set out in these laws are often similar, they are not identical.
16. In the Office's view, it therefore makes sense to clarify the applicable privacy regime and principles in the scheme's legislation. The Office also agrees that the NRAS privacy regime should not add to fragmentation of privacy regulation. A favourable option would be therefore to adopt existing principles in the *Privacy Act 1988* (Cth) as the baseline regulations.
17. This reflects the key theme of national consistency promoted in the Office's submissions to the Australian Law Reform Commission (ALRC) review of privacy laws. The ALRC's Report 108 was released in August 2008 and the Australian Government is now preparing its response.⁷
18. The Consultation Paper outlines a range of options which are discussed in more detail further below (see Proposals 5.1.1–5.2.1). An important issue which the Consultation Paper does not canvass in detail relates to the interaction of the NRAS privacy regime with other existing standards that apply to certain entities.
19. In particular, if the scheme's legislation relies on the National Privacy Principles (NPPs), it should be clarified whether existing Australian Government agencies will remain bound by the Information Privacy Principles (IPPs) when they receive information collected under the scheme. If the ALRC's proposed reforms are adopted, the shift from two sets of principles to one under the Privacy Act may reduce any complexity encountered in the transition phase. In the meantime, these matters could usefully be considered further in a privacy impact assessment.

Privacy impact assessments

20. A systematic way of identifying and resolving a project's privacy and information-handling issues is to conduct a privacy impact assessment (PIA). The Consultation Paper states that: 'Consideration is currently being given to undertaking a Privacy Impact Assessment in 2009.'
21. The Office strongly supports the conduct of a PIA for the scheme, as it involves the collection of considerable amounts of personal information about health practitioners and others, such as complainants. Conducting a formal PIA would further demonstrate the commitment to addressing privacy issues.
22. All parties can benefit from the PIA process, which can:
 - identify any major privacy risks and address them early in the project's development

⁷ See the Office of the Privacy Commissioner's ALRC Inquiry page at www.privacy.gov.au/act/alrc/index.html.

- improve project design, streamline information collection and reduce overlap and red tape, through the examination of initially proposed information flows
- tailor information-handling processes to the project's needs and aims
- increase transparency and public confidence that privacy issues have been properly considered and resolved, and
- reduce the likelihood of 'function creep', which can increase design complexity, diminish public trust and divert a project from its initial aims.⁸

23. In August 2006, the Office released a Privacy Impact Assessment Guide ('PIA Guide') to assist Australian and ACT Government agencies in determining the impact of new proposals on privacy.⁹ The PIA Guide should help the committees of the Australian Health Ministers' Advisory Council (AHMAC) to identify and analyse privacy impacts during the proposal's design phase.¹⁰

24. Once this analysis is complete, a PIA report can be produced summarising the information and making recommendations about how to successfully manage the privacy impacts and project aims. Privacy protections can then be integrated through design, technology, legislative and oversight elements. The Office's responses to specific proposals below highlight some of the areas which could benefit from analysis in the PIA process.

Handling of sensitive information

25. The Consultation Paper states that sensitive information may be collected under the NRAS at various points. Sensitive information is a defined term under the Privacy Act. It includes an individual's health information (also defined), racial or ethnic origin, and criminal record (among other things). All three of these types of sensitive information may be collected under the NRAS. The Office understands that this will particularly relate to practitioners but also to complainants.¹¹

26. The National Privacy Principles (NPPs), and the spirit of the Privacy Act more generally, require that sensitive information be handled with greater

⁸ The term 'function creep' refers to the uncontrolled or unregulated expansion of how databases and information collected for a project are used, particularly when the expansion occurs in ways that the public may not expect or envisage when the project is conceived.

⁹ The Office's PIA Guide is available at www.privacy.gov.au/publications/pia06/index.html.

¹⁰ Practical steps for a PIA include:

- Identifying and defining the project scope and aims;
- Describing and mapping the flows of personal information within the project;
- Identifying and analysing how the project may impact on privacy; and
- Considering options to improve privacy outcomes.

¹¹ See, for example, Consultation Paper, part 2, 'Overview of information required to operate the scheme' (p 5-6).

sensitivity than other personal information.¹² This reflects the high value of privacy that the community places on sensitive information.¹³

27. It is therefore important that any sensitive information is collected, used, disclosed and stored with particular care under the NRAS. For example, it is understood that while conditions on a practitioner's practice would be available on the public register, health information which may related to practice conditions would not be displayed.¹⁴
28. In addition, while consent is usually required to collect sensitive information, this is not necessary if collection is required by law.¹⁵ If the scheme's legislation does require collection of sensitive information such as criminal records (that is, by law), there must be a sound policy basis which weighs up the public interests; and oversight mechanisms should be considered, such as audits, reporting or review.

Secondary uses of practitioners' information

29. A number of the Consultation Paper's proposals relate to secondary uses of information collected under the NRAS. Secondary uses refer to any handling of personal information that is not for the main purpose the information was initially collected. For example, if personal information is primarily collected for registration and accreditation purposes, then any handling of that information for workforce planning or research purposes could be considered a secondary use.
30. Other secondary uses contemplated under the scheme include sharing information with law enforcement bodies; state and territory health authorities; and Australian Government agencies such as Medicare Australia, the Professional Services Review (PSR) and the Department of Immigration and Citizenship (DIAC).
31. The Office submits that all proposals for secondary uses of personal information under the NRAS should be assessed against these criteria:
- What is the purpose of the secondary use, and how closely does it relate to the initial intent of the scheme?
 - Is the secondary use or disclosure necessary and reasonable, with reference to the initial intent of the scheme?

¹² See, eg, NPP 10 under the Privacy Act, which generally requires consent to collect sensitive information unless another exception applies (such as where collection is required by law). See also NPP 2.1(a) on use and disclosure. The NPPs are available on the Office's website at www.privacy.gov.au/publications/npps01.html.

¹³ In the second reading speech for the Privacy Amendment (Private Sector) Bill 2000 (which enacted the NPPs), the then Attorney General, the Hon Daryl Williams, QC, noted that 'the government recognises that the Australian public considers their health records to be particularly sensitive.' Accordingly, 'The bill provides additional protections in relation to the use and disclosure of health information'. (Australian Parliament Hansard, House of Representatives, 8 November 2000, at [http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=\(Dataset:hansardr\)%20Date:08/11/2000;rec=0;orderBy= fragment_number;](http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=(Dataset:hansardr)%20Date:08/11/2000;rec=0;orderBy= fragment_number;))

¹⁴ Public forum on the Consultation Paper, Melbourne, 18 November 2008. See, however, Proposal 4.3.1, discussed below.

¹⁵ See above, note 12.

- Would de-identified information¹⁶ be sufficient?
- Are there adequate limitations and oversight on the scope of the secondary use?
- Does the secondary use align with the reasonable expectations of the health professions, the individuals involved and the community?
- To what extent will individuals be made aware that their information may be used or disclosed in this way (even if it is de-identified)?

Specific proposals for secondary uses are explored further below.

Deidentifying workforce and statistical information

32. The issue of collecting information for workforce planning purposes was the subject of wide-ranging views at the public forum on the Consultation Paper in November 2008. However, there seemed to be widespread agreement about the importance of adequate statistical data for workforce planning purposes. This is reflected in the need to develop a sustainable health workforce, described in the IGA's objectives for the scheme.¹⁷

33. The Office observes that there is no need for such aggregate information to identify individual practitioners. Furthermore, if personal information is adequately de-identified, subsequent privacy issues will be minimised and the Privacy Act will not apply to the information.

34. With those points in mind, the Office believes that:

- information required for statistical purposes should be collected anonymously
- if this is not practicable, personal information collected for this purpose should be de-identified at the earliest available point, and should not be used for any other purposes before it is de-identified
- Special care should be taken in requiring or requesting sensitive information (such as racial or ethnic origin, including indigenous status), noting that individuals may feel more comfortable providing such information on an anonymous basis.

Specific proposals in the Consultation Paper are responded to in Part 2.

Protection of unique identifiers

35. The Office is often consulted about the development and use of unique identifiers. While identifiers are not uncommon or inherently privacy-invasive, there are particular privacy risks around their widespread use which need to be adequately managed (as the Consultation Paper notes,

¹⁶ The term 'de-identified' information is not defined in the *Privacy Act 1988* (Cth). The Office generally uses this term to describe information that has had identifying characteristics removed, to the point where an individual's identity is no longer apparent, and cannot be reasonably ascertained from the information. A distinction can therefore be drawn between 'personal information' as defined and protected by the Privacy Act (section 6), and 'de-identified information', which is not covered by the Privacy Act.

¹⁷ IGA, at para 5.3, objective (e).

p 17). This is reflected in National Privacy Principle (NPP) 7, which limits the adoption, use and disclosure of identifiers issued by the Australian Government, beyond the purpose for which they were created.¹⁸

36. In the context of e-health, the Office has also made submissions to the National E-Health Transition Authority (NEHTA) on privacy issues relating to the Individual Electronic Health Record (IEHR) proposal and its forerunner, the Unique Health Identifier (UHI). These submissions noted the essential need for legislative protections to underpin the e-health system, including to regulate the use of unique identifiers for patients and the 'provider numbers' of practitioners.¹⁹ The Office welcomes the Consultation Paper's recognition that such legislative protections will also be necessary for the NRAS.

Assessing risks and security measures for amalgamated databases

37. The Office has noted the clear public interest in maintaining high safety and quality standards in the Australian health sector, and that the IGA for the scheme supports a nationally coordinated approach to registration and accreditation. It is nevertheless important to identify and minimise any accompanying risks that may arise from the merging of information-handling and storage processes.
38. At present, collection and storage of practitioners' information occurs from disparate sources – the various registration and accreditation boards in each state and territory. This reduces the 'honeypot effect' that can make larger repositories of information attractive. For example, amalgamated databases are more likely to face increased pressure for secondary use proposals (either from governments or the private sector), and can be more attractive targets for hacking and inappropriate data-mining.²⁰ These matters should be considered further in a privacy impact assessment.
39. Relatedly, the Office would also support design features that facilitate appropriate and necessary information flows within the NRAS system (such as between the boards and the national 'agency'), without necessarily requiring that all personal information collected is to be housed in a single 'silo'. Technology and security features can point the way to intelligent privacy solutions in this area, provided they are backed up by privacy-friendly design, legislative protections and oversight measures.

¹⁸ The Office discusses unique identifiers in detail in its submission to the ALRC Review of Privacy, Issues Paper 31, Ch 12, at www.privacy.gov.au/publications/submissions/alrc/c12.html.

¹⁹ See, eg, *Consultation on the Privacy Blueprint – Unique Health Identifiers (Version 1.0); Submission to the National E-Health Transition Authority* (March 2007), paras 7-14 and 54-60, at www.privacy.gov.au/publications/subnehtauhi200703.html. See also, *Consultation on the Privacy Blueprint for the Individual Electronic Health Record; Submission to the National E-Health Transition Authority*, (August 2008) at www.privacy.gov.au/publications/sub_nehta_0808.html.

²⁰ See, eg, The Daily Californian, 'Proposed Student Database Raises Privacy Concerns' (25 January 2005), at www.dailycal.org/article/17359/proposed_student_database_raises_privacy_concerns. See also Department of Homeland Security Privacy Office, *Privacy Impact Assessment for the REAL ID Final Rule* (January 2008), p 6, at www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realidfr.pdf.

Part 2: Comments on specific proposals in the Consultation Paper

40. This part of the submission addresses each of the proposals outlined in the Consultation Paper. Some additional comments are made on issues that may not have been directly addressed in the proposals themselves. Generally, the subheadings in this section reflect those in the Consultation Paper, and the proposals are addressed in the order they were presented.

Information to be collected under the scheme

Information to be collected for initial registration purposes

Proposal 3.1.1: It is proposed that all requests for information will indicate the purposes for which it is being collected.

Office comments

41. The Office supports Proposal 3.1.1. It is good privacy practice and generally a requirement under the Privacy Act that individuals be informed of the purposes for which their information is being collected (among other things). The proposal could be enhanced by noting that all information requests 'must' indicate the purpose of collection, although it is presumed that this is the intention.

Proposal 3.1.2: It is proposed that the national scheme legislation provide for the following key categories of information for the registration of individuals.²¹

Office comments

42. The Office has two main comments on Proposal 3.1.2.

43. *Home address:* If it is necessary to collect home address (in addition to a 'contact address'), the rationale and intended uses should be clarified. The Consultation Paper states that home address is necessary 'In order to properly identify the individual'. However it is unclear how home address would improve identification beyond the other information listed in the proposal, such as name, contact address, date of birth and registration details.

44. *Criminal records:* The Office suggests that boards be given limited discretion to formulate their own policies regarding criminal record checks for practitioners. These policies should be based on necessity and assessed risk and be subject to Ministerial oversight. Inquiries should be limited to the types of offences relevant to public safety or capacity to maintain professional conduct, such as convictions relating to assault, illicit drugs, offences involving children and other serious offences. The

²¹ In summary: name and contact details; date of birth; qualifications; overseas registration details; details of recency of practice and other requirements; criminal record; professional indemnity insurance; registration details (Consultation Paper, pp 6-7).

relevance of some offences may be affected by how recently they were committed. Spent convictions legislation may also apply.²²

45. Another consideration is whether criminal record information needs to be stored once checked, beyond a 'Yes/No' type response as to whether any serious offences have been committed over the relevant timeframe. This may be relevant to electronic checking as outlined at 7.10. A 'Yes' response could prompt further investigation, though in many case details may not need to be stored. The privacy impact assessment (PIA) should look at various models including in Western Australia, where the Office understands criminal record checks can occur with medical practitioners' consent, but detailed information is not recorded on the register.²³

Employer details

Proposal 3.2.1: *It is proposed that the national scheme legislation provide the boards with the power to collect employer details and other similar details in order to enable notification by the relevant board to employers when a practitioner's registration status changes or conditions are placed on practice.*

There are two options to give effect to this arrangement:

Option 1: *Require name and address of employer, public health organisations, private hospitals, day procedure centres or nursing homes at which the practitioner is accredited to be recorded on registration and updated on renewal.*

Option 2: *Provide the boards with a power to require the practitioner to provide these details to the board, as necessary.*

Office comments

46. The Office prefers Option 2 over Option 1, provided that there is adequate oversight of boards' discretion. Option 2 will empower boards to collect employer information only to the extent necessary for the profession's circumstances (including by limiting in the legislation the type of information that boards may require under this provision). Limiting information collection to what is necessary reflects good privacy practice. Such an option is also likely to be less onerous for practitioners.

The unique identifier

Proposal 3.3.1: *It is proposed that the legislation require that each registered health practitioner be allocated a unique identifier in the new registration system.*

Office comments²⁴

47. The Consultation Paper notes some of the privacy issues associated with unique identifiers (p 17). The paper refers to consultation with the National E-Health Transition Authority (NEHTA) and Medicare Australia in developing the format for any unique identifier used in the system. The Office suggests that the Privacy Commissioner also be consulted on these

²² The Privacy Commissioner has some responsibilities in this area under the *Crimes Act 1914* (Cth), see www.privacy.gov.au/act/convictions/index.html. There are separate State/Territory schemes.

²³ See Consultation Paper, Table p 24, 'Publicly available content of current registers – Medical'.

²⁴ See also paras 35-36 above.

developments, and the necessary safeguards to protect the use of identifiers.

***Proposal 3.3.2:** It is proposed that the national scheme legislation authorise NEHTA and Medicare Australia, to adopt, use and disclose the unique identifier allocated to practitioners in order to enable e-health developments and other information sharing in the public interest. It is further proposed that the legislation governing the operation of NEHTA and Medicare Australia provide appropriate protection for the information provided to these agencies by the national scheme.*

Office comments

48. Acknowledging the general intent of Proposal 3.3.2, the Office believes the reference to 'other information sharing in the public interest' is too broadly expressed. The scheme's legislation should state in more detail the purposes for which NEHTA and Medicare Australia can adopt, use and disclose the unique identifier. As Proposal 3.3.2 goes on to suggest, this should be reinforced by legislation governing NEHTA (and/or e-health generally) and Medicare Australia's operations. See also proposal 7.1.1.

Identity checking on initial registration

***Proposal 3.4.1:** It is proposed that the national scheme legislation provide a power for boards to require identity checking, through photo identification and a "100 point check" system.*

There are three options to give effect to this arrangement:

***Option 1:** All boards to require identity checking on initial registration post 1 July 2010, but not for existing registrants.*

***Option 2:** Boards to decide whether identity checking along the lines of Option 1 will be required in their profession.*

***Option 3:** Boards to decide whether identity checking along the lines of Option 1 will be required for only some applicants for registration.*

Office comments

49. Similarly to its position on Proposals 3.1.2 (criminal records) and 3.2.1 (employer details), the Office believes that boards should be given limited discretion to decide the extent to which identity checking is necessary within their profession. If boards are given such discretion, they should be required to develop policies based on necessity and risk assessment. This would go against Option 1.

50. In determining the favoured option for this proposal, the scope of identity fraud within the professions should be examined, and existing practices for identity-checking should be assessed for their utility. For example, identity-checking may be more privacy invasive where it involves the retention of identity records, rather than simply recording that a practitioner has met the requisite standard.²⁵ These could be relevant matters to be examined in a privacy impact assessment (PIA) for the scheme.

²⁵ See, eg, Office of the Privacy Commissioner of Canada, *Collection of Driver's Licence Numbers Under Private Sector Privacy Legislation: A Guide for Retailers* (December 2008), at www.privcom.gc.ca/information/pub/guide_edl_e.asp.

Information to be collected for workforce planning purposes

Proposal 3.8.1: *It is proposed that the national scheme legislation provide for the Ministerial Council to specify from time to time, certain data items that must be collected as part of registration and renewal of registration processes where these data items are needed for workforce planning purposes as long as there is a clear need for the data and it is not too burdensome. Note that provision will also be made for additional data to be collected on a voluntary basis.*

Proposal 3.8.2: *It is further proposed that the current voluntary paper-based labour force surveys conducted by current boards on behalf of jurisdictions be discontinued.*

Proposal 3.8.3: *It is further proposed that information collected purely for workforce planning purposes will not be made available for board/agency purposes.*

Office comments (Proposals 3.8.1–3.8.3)²⁶

51. If the registration process is found to be an appropriate time for collecting workforce planning data, the Office's starting point is that such statistical information does not need to identify individuals. Accordingly, if practicable this information should be collected anonymously, even if registrants are given an option to pre-populate data from their record (that is, any link to the registrant's record should be broken at the point of collection).
52. Special care should be taken in any requirement to collect sensitive information such as country of birth, indigenous status or citizenship characteristics. Anonymity in this context would build confidence and be privacy-enhancing (noting that properly de-identified information is not personal information and therefore does not come under the Privacy Act's jurisdiction).
53. The Office submits that year of birth is an adequate indicator for statistical purposes, rather than date of birth as the Consultation Paper suggests.
54. The Office supports the criteria in Proposal 3.8.1 that there must be a clear workforce planning need for each data item collected, and that the process should not be too burdensome.
55. If workforce planning information is collected on an identifiable basis, the Office agrees that such information should not be made available for board/agency purposes, nor to any other entity beyond the Australian Institute of Health and Welfare (AIHW) or relevant statistical coordinator.

Public availability of de-identified workforce planning statistics

Proposal 3.8.4: *It is proposed that the national scheme legislation provide for the Ministerial Council to require that specified, de-identified information is provided to the Council and any of its committees for workforce planning analysis.*

Proposal 3.8.5: *It is proposed that the national scheme legislation requires that de-identified information relevant to workforce planning is made publicly available in a timely manner and by suitable means.*

²⁶ See also paras 32 to 34 above.

Office comments

56. Provided that statistical information is sufficiently de-identified, so that no individual registrant's identity is reasonably ascertainable from a combination of the data, the Office does not oppose the public availability of such de-identified workforce information. Although the Privacy Act will not apply to such information once it is de-identified, it would be appropriate to notify registrants of the purposes for which the information is being collected and the likely uses and disclosures of that information.

Publicly available information

Information on the public register

Proposal 4.1.1: *It is proposed that the national scheme legislation specify that the following categories of information in relation to each registrant are available on the public register:*

- | | |
|---|---|
| (a) Current name | (g) Class of registration (where relevant) |
| (b) Sex | (h) Division (where relevant) |
| (c) Postcode of contact address and name of postcode area | (i) Conditions on practice (where relevant) |
| (d) Registration identifier | (j) Date of suspension and date suspension is to end (where relevant) |
| (e) Date of first registration | (k) Endorsed specialities (where relevant) and |
| (f) Renewal date | (l) Other endorsements (where relevant). |

Office comments

57. The Office acknowledges the potential public safety benefits of listing relevant personal information about practitioners on the public register for consumers and employers. Comments on specific items follow.

58. *Postcode and suburb:* The Office believes it is appropriate to list these items rather than full business address due to potential privacy risks. If there is a strong preference from particular professions for listing full address, the Office believes that should be a voluntary item only.

59. *Registration identifier:* The Consultation Paper does not spell out the utility of publicly listing practitioners' registration identifiers. As the Paper notes, there can be specific privacy risks associated with unique identifiers. The privacy impact assessment should examine the benefits and any privacy risks of making this identifier widely available.

60. *Conditions on practice:* This item should be limited to current, work-related conditions on practice and should not disclose health information about the practitioner. Care should be taken in phrasing the relevant practice conditions to avoid inferences as to health conditions, as far as practicable. In line with the Privacy Act's data quality requirements, this and other information should be kept accurate, complete and up-to-date.²⁷

61. *Date of suspension and end date:* This item should only relate to current suspensions and should be removed once a registrant is reinstated. As

²⁷ See, eg, National Privacy Principle (NPP) 3 and Information Privacy Principle (IPP) 8.

noted above, such information should be kept accurate, complete and up-to-date.

De-registered practitioners

There are four options for recording de-registered practitioners.

Option 1: *De-registered practitioners could appear on the register with a status of de-registered.*

Option 2: *De-registered practitioners could be removed from the public register.*

Option 3: *Practitioners de-registered for conduct reasons could appear on a separate register of de-registered practitioners.*

Option 4: *Practitioners de-registered for conduct reasons could continue to be shown on the public register with the status of de-registered for conduct reasons.*

Proposal 4.2.1: *It is proposed that the national scheme legislation provide that Option 4 be adopted and that the names of practitioners de-registered for conduct reasons appear on the public register with an indication that they have been de-registered for conduct reasons.*

Office comments

62. The Office supports Option 4. It seems appropriate that practitioners who are de-registered for conduct reasons be distinguishable from those who simply retire or decline to renew registration. The amount of information provided should be limited to what is necessary for public safety.
63. If consideration is being given to displaying information about individuals who were deregistered prior to the scheme's commencement (planned for 1 July 2010), reference should be made to how existing boards handle this information; what individuals and the public might reasonably expect regarding how such information already held should be handled; and issues of retrospectivity.
64. Some of the above considerations will also be relevant in determining how long information about deregistration should remain publicly available, or how else older information should be stored. For example, the Privacy Act requires information be destroyed or de-identified when it is no longer needed. This may be a consideration for a privacy impact assessment.

Recording of conditions on practice

Proposal 4.3.1: *If conditions on practice relate to practitioner health or impairment issues, it is proposed that the national scheme legislation provide that the public register record that a health condition applies, with no further details appearing on the register. However, if specific restrictions on professional practice apply, they would appear on the register.*

The agency could release information about health conditions in particular circumstances if it was judged to be in the public interest but the test would be a high one.

Office comments

65. The Office does not support Proposal 4.3.1, to the extent it suggests that health information about registrants be publicly disclosed on the register. This does not appear necessary for public safety and does not reflect existing practices in most states and territories.²⁸
66. The Office does agree that specific restrictions on professional practice may be appropriate to disclose on the register if this is necessary for public safety. However, if the information is relevant to employers (or potential employers) only, then the information should not be publicly displayed and should be communicated to employers by other means.
67. As noted above, care should be taken in phrasing the relevant work restrictions, to avoid inferences as to health conditions as far as practicable.
68. The Office agrees that any disclosure of sensitive information without consent would require a high test. The reference to releasing information about registrants' health conditions in the public interest would require a number of considerations. These include what notice is given to practitioners when the information is collected, and their subsequent expectations; whether consent could be sought for the disclosure; whether the disclosure would lessen a serious and imminent threat to someone's life, health or safety; or is required or authorised by law. These and other exceptions are found in the general use and disclosure provisions under the Privacy Act (see, for example, National Privacy Principle 2).

Release of public register information

Proposal 4.5.1: It is proposed that there be a general power in the national scheme legislation to allow any person to obtain a copy of, or an extract from, the register on payment of the fee determined by the agency. It is proposed that the agency would have a power to refuse to provide a copy of the register to any person unless satisfied that it is in the public interest to do so.

Office comments

69. The Office generally supports Proposal 4.5.1, on the proviso that appropriate safeguards (legislative and otherwise) are placed around the ways that information on the register may be collected, used and disclosed. The Office supports measures to prevent this information being used for marketing and other commercial purposes which may not relate to public safety.
70. The legislation should specify protections around the subsequent use of information derived from the register that are enforceable and auditable. These protections should prevent the compilation of register information into a separate database that may not be as closely regulated. Options may be canvassed in a privacy impact assessment.

²⁸ Consultation Paper, Table p 24, 'Excluded information'.

Public access to the findings of formal proceedings

Proposal 4.6.1: *It is proposed that the national scheme legislation provide for the publication of tribunal decisions relating to registrants where it is in the public interest to do so.*

Proposal 4.6.2: *There is a public interest in making board or committee decisions in relation to conduct matters public. It is proposed that decisions be published on the register of decisions on the agency's website.*

There are two options to give effect to this arrangement:

Option 1: *All conduct decisions of boards or committees are published (with patient details de-identified).*

Option 2: *Boards may order that certain decisions are confidential and order that the decision register contain a confidential information notice.*

Office comments

71. The assessment and implementation of these proposals should strike an appropriate balance between public safety and personal privacy. The Office agrees that publication of tribunal decisions is appropriate where this is in the public interest, subject to confidentiality requirements in particular cases. Option 2 in Proposal 4.6.2 is preferred.
72. The Office submits that all patient details should be removed from decisions before publication. This includes where reference to a particular clinic, town, health conditions or personal characteristics (such as Indigenous status) may reveal a patient's identity when combined, without actually naming them.
73. The Office agrees that performance management and health management decisions are of a different nature to tribunal decisions, and should not be published.
74. In this era of electronic communication, a relevant consideration for a privacy impact assessment could be whether any additional privacy risks arise from having tribunal decisions being made more easily available and searchable online, and collated in a single location.
75. Old tribunal decisions should be removed or permanently de-identified if they are no longer needed for a relevant purpose (p 14 of the Consultation Paper refers). Boards would need to consider their privacy obligations in this regard. For example, National Privacy Principle 4.2 and any specific requirements under the scheme's legislation or policies.

The privacy regime

Legislative options

Option 1: Using an existing privacy law

- (a) *Use the private sector provisions of the Privacy Act 1988*
- (b) *Use the public sector provisions of the Privacy Act 1988*
- (c) *Use an existing State or Territory law*

Option 2: A bespoke privacy law

Proposal 5.1.1: *It is proposed that the national scheme legislation use the private sector provisions of the Privacy Act 1988 as the basis for the privacy arrangements in the national scheme.*

Proposal 5.2.1: *It is proposed that the existing Commonwealth private sector privacy regime and National Privacy Principles are incorporated by reference into the national scheme legislation.*

Office comments (Proposals 5.1.1 and 5.2.1)

76. The Office supports the adoption and incorporation of the National Privacy Principles (NPPs), or future equivalent, by reference (as amended from time to time). The Office also supports the Australian Privacy Commissioner's role as privacy complaint-handler for the scheme.
77. The Office agrees it is preferable to rely on existing privacy standards rather than a 'bespoke' privacy law. A separate set of specific principles would contribute to regulatory fragmentation while potentially overlapping with many of the general obligations under the Privacy Act (perhaps in modified form).
78. Where additional, specific protections are needed beyond the principles-based standards of the NPPs, the Office supports those protections being specified under the scheme's legislation. For example, specific protections around use of information from the public register, officer confidentiality provisions and protections around the unique identifier.²⁹
79. The Office notes that some jurisdictional details will need to be clarified. For example, the status of the 'national agency'; and interactions between the NRAS and Australian Government agencies that are already bound by the Information Privacy Principles (IPPs). Such agencies include the AIHW, Department of Immigration and Citizenship (DIAC), Professional Services Review (PSR) and Medicare Australia. These issues should be examined in the privacy impact assessment.

²⁹ See the Consultation Paper, sections 4, 6 and 7 respectively.

Information sharing

Enabling e-health developments

Proposal 7.1.1: It is proposed that the national scheme legislation prevents the adoption of the scheme's health practitioner identifier for other purposes by other bodies. The legislation would also need to exempt the adoption and use of the identifier for e-health purposes subject to legislation providing appropriate protections being in place to oversight such e-health activities.

Office comments³⁰

80. The Office supports Proposal 7.1.1, and agrees that appropriate legal protections and oversight are needed around the handling of any unique identifier developed for the scheme. This aligns with the intent of National Privacy Principle (NPP) 7, which restricts the use of Australian Government-issued identifiers generally, due to specific privacy risks around their use.
81. There are a number of reasons why specific protections are likely to be needed in the scheme's legislation beyond NPP 7. Firstly, NPP 7 only binds some private sector organisations and does not affect government agencies. Secondly, NEHTA and Medicare Australia's proposed adoption and use of the identifier would be unlikely to satisfy the requirements for 'prescribed' exceptions under NPP 7.³¹ Thirdly, defining the scope of exceptions which allow the use of identifiers in legislation provides an appropriate degree of parliamentary oversight.
82. The Office would welcome further consideration and consultation should on the extent of information-sharing about registrants under the e-health scheme as it develops (Consultation Paper refers, p 17, para 3), and the proper provision of notice to practitioners on such matters.
83. Overall, the privacy impact assessment for the NRAS should examine the detailed steps necessary to protect the scheme's identifier, and the Privacy Commissioner should continue to be consulted on these issues.

Research

Proposal 7.2.1: It is proposed that the national scheme legislation provide for de-identified information from the registration system to be available to government agencies and to appropriate classes of other persons for research and statistical purposes.

Office comments³²

84. The issues relevant to Proposal 7.2.1 are comparable with Proposals 3.8.4 and 3.8.5 above (workforce planning). However, the current proposal is distinguishable because it relates to secondary use of registration

³⁰ See also proposals 3.3.1-3.3.2.

³¹ See subsection 100(2) of the *Privacy Act 1988* (Cth).

³² On secondary uses generally, see paras 29 to 31 above.

information for research, rather than information specifically collected for workforce planning purposes.

85. The Privacy Act will not apply to statistical information that is sufficiently de-identified so that no individual registrant's identity is reasonably ascertainable. Nevertheless, it would be appropriate to notify registrants of the purposes for which the information is being collected and the likely uses and disclosures of de-identified information derived from it.
86. Although the Privacy Act does not prevent such handling, the views of the professions will also be instructive on this proposal, particularly as it refers to research beyond workforce planning purposes. For example, the Office understands there are considerable reservations in the wider community about the use of health information (more specifically) for the secondary purpose of research, even once it is de-identified.³³

Professional Services Review Scheme (PSR Scheme)

Proposal 7.3.1: It is proposed that the national scheme legislation governing the release of information by the agency and the boards will set out the circumstances when material will be forwarded to the PSR.

Office comments

87. The Office recognises the need to continue existing linkages between the PSR Scheme and registration bodies.³⁴ Any expansion of such information-sharing between registration boards and the PSR should be based on (and limited to) what is necessary, with reference to public safety and the role of the PSR. National Privacy Principle (NPP) 2 permits the use or disclosure of personal information where required or authorised by law. It is therefore important to have a sound policy basis for any disclosures of this nature that are authorised by the scheme's legislation.
88. Accordingly, disclosures should also satisfy criteria as to likelihood and seriousness of a public health risk, which disclosure to the PSR would avert. Registrants should also be notified of the potential for information to be shared with agencies such as the PSR, and for what purposes.
89. A further, fundamental issue is whether specific provision in the scheme's legislation is necessary for such purposes (this is also relevant to proposals 7.4.1, 7.5.1 and 7.7.1 below). The Office notes that NPP 2 has provisions on disclosure for law enforcement and protection of the public revenue. Current proposals suggest that the scheme will incorporate the NPPs by reference. It would be useful to clarify whether the general exceptions under NPP 2 would apply to the personal information held by the national agency and boards.
90. If so, it should be examined whether NPP 2 exceptions (particularly 2.1(f) and (h)) are in themselves sufficient to permit disclosure to relevant authorities where 'unlawful activity' or 'seriously improper conduct' is

³³ 53% of women surveyed said consent should be sought, as did 43% of men surveyed. See the Office of the Privacy Commissioner, *Community Attitudes to Privacy 2007*, p 46, available at www.privacy.gov.au/publications/rcommunity07.pdf.

³⁴ Consultation Paper, p 17 refers.

suspected. Alternatively, it may be clearer to specify the scope and limits of such disclosures in the scheme's legislation. All of these matters could be examined in a privacy impact assessment.

Medicare Australia

Proposal 7.4.1: It is proposed that the national scheme legislation governing the release of information by the agency and the boards enables the release of information to Medicare Australia and specifies the purposes for which the information is to be released.

Office comments

91. The Office sees merit in specifying the circumstances in which information from the NRAS may be disclosed to Medicare Australia under the scheme's legislation. The Office submits that any expansion of existing information-sharing between registration boards and Medicare Australia must satisfy criteria of relevance to Medicare Australia's functions and necessity of sharing the information. Many of the considerations raised above for Proposal 7.3.1 are also applicable here.

92. In addition, the prospect of '[sharing] information at the pre-finding stage' requires careful assessment.³⁵ Relevant considerations include:

- what threshold of risk might make such disclosures appropriate;
- any potential cumulative impacts on practitioners' privacy as a result of information dissemination and multiple ongoing investigations; and
- the views of Medicare Australia and the professions.

Overseas trained practitioners

Proposal 7.5.1: It is proposed that the privacy framework to apply to the agency authorise the disclosure of relevant information to the DIAC for purposes under the Migration Act 1958.

Office comments

93. This proposal is broadly phrased in reference to purposes under the Migration Act, and more detail would be useful to fully assess it. As in relation to the PSR and Medicare Australia, limiting such disclosures to those which are necessary and relevant is a key consideration. Adequate notice would also need to be provided to relevant individuals when they register or renew.

94. The extent to which information-sharing with DIAC could impact on privacy should be assessed in the privacy impact assessment (PIA). Further consultation, including with DIAC and the Privacy Commissioner, may also be of assistance. For example, would personal information be constantly shared as a matter of course, or upon request by DIAC during an investigation? Also, if it is intended that NPP 2 will apply to information

³⁵ Consultation Paper, p 18 refers.

held by the boards and agency, is specific legislative provision required here? (See Office comments under 7.3.1).³⁶

State and Territory government health bodies

Proposal 7.7.1: It is proposed that the national scheme legislation enable the sharing of de-identified information with State and Territory government bodies for specified purposes and the notification of identified practitioners who pose a public health risk.

Office comments

95. This proposal has two distinct issues, outlined below.

96. *Disclosure of de-identified information to State and Territory bodies:* The Privacy Act does not apply to de-identified information and privacy concerns about such information are markedly reduced. However there are two comments worth noting on this part of the proposal. Firstly, it is important that the information is indeed properly de-identified.³⁷ Secondly, adequate notice should be provided to individuals that their information may be de-identified and used for such secondary purposes in future.

97. The Consultation Paper notes that sharing de-identified information with state and territory entities would be important, for example, in relation to health service delivery and drugs and poisons matters (p 19). The paper does not articulate further specifics, such as how this might differ from the workforce planning information that is proposed to be publicly available under Proposals 3.8.4 and 3.8.5. This could be clarified.

98. *Notification of public health risks:* There is limited detail on the specifics of this part of the proposal. The Office acknowledges the public interest in appropriate information flows which protect the public from serious health risks. However, the Consultation Paper does not outline the process for such disclosures or the threshold definition of a 'notifiable public health risk'.³⁸

99. It is not clear the extent to which 'public health protection bodies' here might differ from State and Territory health departments discussed in the following Proposal 7.8.1.³⁹ A possible option for consideration is whether it would be necessary to alert state bodies other than the relevant health department about 'notifiable public health risks'; or whether the health department is an appropriate conduit for initial discussion of such matters, to determine whether any other state authorities should be involved.

³⁶ Paragraph 89 above.

³⁷ See paragraph 72 above, and paragraphs 32 to 34.

³⁸ It may be that the brief treatment of disclosures to public health bodies in the Consultation Paper is a result of previous consideration of this issue in the complaints arrangements consultation paper (Consultation Paper, p 19 refers), although the Office was not involved in those consultations.

³⁹ Arrangements for 'health complaint bodies' are also discussed separately to 'public health protection bodies' in the Consultation Paper, part 7.6.

Notification to Commonwealth, State and Territory health departments

Proposal 7.8.1: It is proposed that the national scheme legislation provide that whenever a board identifies that the health of a patient who is not directly involved in a case under investigation may have been adversely affected by a practitioner, the board must notify the relevant State or Territory health department so that remedial action can be taken.

Office comments

100. As noted immediately above, the Office acknowledges the public interest in appropriate information flows which protect the public from serious health risks. The Office has two further comments on this proposal.
101. Firstly, it should be considered whether 'may have been adversely affected' is a high enough threshold for warranting notification of the relevant State or Territory health department.
102. Secondly, the Office suggests that the scheme's legislation could empower (rather than require) the boards to disclose practitioner and/or patient information to the relevant health department, provided the appropriate risk threshold is met. This would provide an additional check on necessity and control over information flows between boards and State or Territory departments.

Law enforcement agencies

Office comments

103. Although it is not expressed as a proposal, the Consultation Paper states that 'The national scheme legislation will provide a general power to share information with law enforcement bodies.' (Part 7.9) The paper states that such disclosures may or may not relate to enforcement of the NRAS.
104. As outlined in response to Proposal 7.3.1, National Privacy Principle (NPP) 2 provides general authorisations to share information with law enforcement bodies subject to certain criteria (see NPP 2.1(f) and (h)). The relationship between the scheme's legislation and the use and disclosure provisions under the NPPs (if incorporated by reference) should be clarified. Any specific provisions in the scheme's legislation should be at least as robust as the standards required by NPP 2.1(f) and (h). The NPPs recognise the seriousness of disclosures for law enforcement purposes by requiring organisations to make a note of any disclosure under NPP 2.1(h).
105. The Office submits that sharing of information with law enforcement agencies under the scheme (and possibly with DIAC) should be subject to review, including reporting to and oversight by the Ministerial Council.⁴⁰ This would be a valuable safeguard against 'function creep' of the NRAS database beyond the purposes initially contemplated or agreed. This is

⁴⁰ The IGA states (at 10.2) that 'The national agency will submit an annual report to the Ministerial Council.' These reports will then be tabled in the respective Parliaments.

particularly relevant if disclosures do not relate to enforcing the NRAS itself.

Trans-Tasman Mutual Recognition

Proposal 7.12.1: It is proposed that the national scheme legislation make appropriate provisions to cover the sharing of information with New Zealand registration authorities consistent with the TTMRA.

Office comments

106. Information sharing with New Zealand registration authorities appears consistent with the requirements of the TTMRA as outlined in the Consultation Paper.

107. It should be noted that National Privacy Principle (NPP) 9 regulates, but does not prevent, transborder information flows in the private sector (and potentially under the proposed scheme). In brief, NPP 9 permits overseas transfer of personal information if one of these conditions apply:

- equivalent privacy protections exist in the host country (this would include New Zealand) or assurances that the information will be treated consistently with the NPPs;
- individual consent;
- contractual requirements that are in the individual's interests; or
- consent is impracticable and certain other conditions are satisfied.

108. If the NPPs are incorporated into the NRAS by reference, it would still be appropriate to outline more specific arrangements between Australian and New Zealand registration authorities under the scheme's legislation. These arrangements could operate in addition to the baseline requirements of NPP 9.

109. It is also relevant to note that the Office has an agreement with the Office of the Privacy Commissioner in New Zealand – to enhance the exchange of information and cooperation between the two agencies, and to promote cross-border cooperation in investigation and enforcement.⁴¹

Overseas regulatory authorities

Proposal 7.13.1: It is proposed that the national scheme legislation give boards powers to exchange information with international registration bodies.

Office comments

110. Such powers should be limited to exchange of necessary information, which may be reflected in current agreements relating to cooperation with overseas health regulatory bodies.⁴² See also paragraphs 107-108 above.

⁴¹ See Office of the Privacy Commissioner media release, 27 August 2008, 'Australia & New Zealand – privacy regulators sign agreement', at www.privacy.gov.au/news/media/2008_27.html.

⁴² Consultation Paper, p 20 refers.

Health records

Proposal 8.1: It is proposed that the national scheme legislation make the boards the repository of last resort with the power to take possession of patient health records when a practitioner has defaulted on their obligations.

Office comments

111. The Office acknowledges the problems presented by abandoned medical records and the potential for inadequate record-handling following practice closures. However, the Office does not support Proposal 8.1. This is on the basis that the handling of patient records is a separate issue beyond the ambit of the NRAS, and is better addressed in other ways.
112. For example, in submissions to the recent Australian Law Reform Commission (ALRC) review of privacy, the Office supported amendments to the Privacy Act which would create new obligations around transfer of patient records and health service closures.⁴³ The ALRC's final Report 108 recommended such amendments.⁴⁴ The Australian Government is currently preparing its response to that Report. It is hoped that those provisions, if enacted, would address some of the problems identified in the Consultation Paper.

Transitional issues – Supply of information from existing boards to the agency (Consultation Paper part 9.1)

Office comments

113. It is important that appropriate information-handling is required during the scheme's transitional phase, because some states and territories do not have specific privacy protections, and the legal framework of state-based registration boards means that the Privacy Act may not apply to them. Accordingly, it may be appropriate to require compliance with the National Privacy Principles (NPPs) by contractual means, particularly where equivalent or similar protections would not otherwise apply.

⁴³ See the Office of the Privacy Commissioner, Submission to ALRC Discussion Paper 72 (December 2008), response to Proposals 57-7 and 57-8, at www.privacy.gov.au/publications/submissions/alrc_72/PartH.html#apr22.

⁴⁴ See ALRC, Report 108 (August 2008), Recommendations 63-7 and 63-8, at www.austlii.edu.au/au/other/alrc/publications/reports/108/63.html.

Conclusion

114. Overall, the Office welcomes the considerable attention to privacy issues in the development of the National Registration and Accreditation Scheme for the Health Professions. Through a comprehensive privacy impact assessment and further consultation, the public safety objectives of the scheme can be achieved in a way that respects and protects the privacy of health practitioners. This approach would recognise the valuable services these practitioners provide to the Australian community, with the support of the registration and accreditation boards.
115. The Office looks forward to further opportunities for public consultation, including an exposure draft of the second tranche of legislation once policy directions are finalised, and will work to provide further privacy advice on the scheme as it is developed and implemented.