Australian Government

Office of the Privacy Commissioner

Inquiry into the National Registration and Accreditation Scheme for doctors and other health workers

Submission to the Senate Community Affairs Committee

April 2009

Key Recommendations

1. The Office of the Privacy Commissioner (the Office) welcomes the opportunity to provide comments on the development of the National Registration and Accreditation Scheme for the health professions (NRAS). The Office has previously made an extensive submission to the Australian Health Ministers' Advisory Council (AHMAC) on the NRAS proposal.

2. The Office also appreciates the opportunity to participate in public forums as part of the consultation process in the development of the NRAS.

3. It is the Office's view that privacy has an integral part to play in the NRAS. In particular, the Office believes that the NRAS should protect practitioners' privacy through sound information handling practices.

4. The Office's recommendations are to:

- adopt and incorporate the National Privacy Principles, or future equivalent, by reference in the NRAS legislation
- have the Australian Privacy Commissioner as the privacy complaint-handler for the NRAS
- conduct Privacy Impact Assessments to assist in identifying any major privacy risks and addressing them early in the project's development
- limit the proposed criminal history checks to the types of offences relevant to public safety or capacity to maintain professional conduct
- assess all proposals for secondary uses of personal information under the NRAS against a set of specified criteria
- collect information required for statistical purposes in a de-identified form, or if not practicable, de-identifying personal information at the earliest available point
- identify a clear workforce planning need for each data item collected under the NRAS
- consult the Privacy Commissioner on the development of unique identifiers, including on any proposed safeguards to protect the use of identifiers.

Office of the Privacy Commissioner

5. The Office of the Privacy Commissioner (the Office) is an independent statutory body whose purpose is to promote and protect privacy in Australia. 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, all private health service providers and some small businesses.

Overview

6. The Office supports the development of the NRAS and welcomes the focus given to privacy issues in the development of the NRAS. Through a comprehensive privacy impact assessment, and further consultation, the Office believes that the public safety objectives of the NRAS can be achieved in a way that respects and protects the privacy of health practitioners.

7. The Office welcomes the opportunity to provide further input into the development of the NRAS. The Office participated in the NRAS public forum held in November 2008. In December 2008, the Office made a submission to AHMAC regarding proposed arrangements for information sharing and privacy for the NRAS.[1]

8. The Office looks forward to further opportunities for public consultation, including exposure drafts of future legislation, and will provide further privacy advice on the NRAS as it is developed and implemented.

9. In this submission, the Office briefly outlines the major privacy considerations that can be usefully incorporated into the development of the NRAS. These issues are discussed in more detail below.

Implementing an appropriate privacy regime

10. The Office considers it critical that privacy protections are examined and built in from the beginning of a project's development. The framework of privacy regulation and governance arrangements are a fundamental consideration for the NRAS. Decisions on these will determine what standards of privacy and information-handling will be required under the scheme, how privacy issues will be regulated and by whom.

11. The Office's *Community Attitudes Survey 2007* revealed a very high level of trust in health service providers – more than any other sector.[2] The NRAS will provide an opportunity to reinforce that trust by maintaining professional standards.

12. Generally, the activities of Australian Government agencies, large private sector organisations and all private health sector professionals are regulated by the Privacy Act. However, as the NRAS is an intergovernmental project crossing jurisdictions it is important that there be consistent protection for the personal information handled as part of the NRAS.

[1] http://www.privacy.gov.au/publications/sub_nras.html

[2] 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.

13. As the Consultation Paper on *Proposed arrangements for information sharing and privacy* (Consultation Paper[3]) points out, there are different laws which regulate privacy at the federal and (some) State and Territory levels. In the Office's view, it therefore makes sense to clarify what privacy regime will apply, and considers that the NRAS privacy regime should not add to the fragmentation of privacy regulations.

14. Since 2005[4] the Office has been promoting the concept of national consistency in privacy regulation. In the Office's submission to the Australian Law Reform Commission's Review of Privacy – Discussion Paper 72 [5] the Office agreed that the Privacy Act should be amended to consolidate the current Information Privacy Principles and National Privacy Principles (NPPs) into a single set of principles that would be generally applicable to agencies and organisations, subject to exceptions as required. The Office also agreed that the NPPs should provide the general template in drafting and structuring the proposed unified privacy principles.

15. The Office considers that the best option for the NRAS would be to adopt the existing principles in the Privacy Act as the baseline regulations. The Office supports the adoption and incorporation of the NPPs, or future equivalent, by reference in the NRAS legislation.

16. The Office also supports the Australian Privacy Commissioner's role as privacy complaint-handler for the NRAS.

Privacy Impact Assessments

17. As the NRAS involves the collection of considerable amounts of personal information, the Office strongly supports the conduct of Privacy Impact Assessments (PIA). PIAs provide a systematic way of identifying and resolving a project's privacy and information-handling issues. Conducting a formal PIA would also further demonstrate the commitment to addressing privacy issues.

18. 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.[6] The PIA Guide could assist AHMAC to identify and analyse privacy impacts during the proposal's design phase.

19. The PIA process can identify any major privacy risks and address them early in the project's development. It can also streamline information collection through the examination of initially proposed information flows. Additionally, a PIA will increase transparency and public confidence that privacy issues have been considered as well as allow information-handling processes to be tailored to the project's needs and aims.

Criminal history checks

20. On 5 March 2009, AHMAC agreed that the NRAS will require mandatory criminal history checks for all health professionals registering for the first time in Australia. All

[3] 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.
[4] http://www.privacy.gov.au/act/review/index.html
[5] http://www.privacy.gov.au/publications/alrc211207.html
[6] The Office's PIA Guide is available at www.privacy.gov.au/publications/pia06/index.html.

other registrants will be required to make an annual declaration on criminal history matters when they renew their registration.

21. The Office believes that the proposed criminal history checks 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 relevance of some offences may also be affected by how recently they were committed. Spent convictions legislation may also apply.[7]

22. 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. For example, a 'Yes' response could prompt further investigation, though in many cases details may not need to be stored.

23. As the NRAS will require the collection of criminal history information, the Office suggests that oversight mechanisms such as audits, reporting and review should be considered.

Secondary uses of practitioners' information

24. 'Secondary use' refers to any handling of personal information that is not for the main purpose for which the information was initially collected. For example, if personal information is primarily collected for registration and accreditation purposes under the NRAS, then any handling of that information for workforce planning or research purposes could be considered a secondary use.

25. The Office submits that all proposals for secondary use 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 NRAS?
- Is the secondary use or disclosure necessary and reasonable, with reference to the initial intent of the NRAS?
- Would using de-identified information[8] be sufficient?
- Are there any 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)?

[7] 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.

[8] 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.

De-identifying workforce and statistical information

26. At the public forum on the Consultation Paper in November 2008, there appeared to be widespread agreement about the importance of adequate statistical data for workforce planning purposes.

27. In order to minimise privacy concerns, the Office believes that information required for statistical purposes should be collected in a de-identified form. If this is not practicable, personal information collected for this purpose should be de-identified at the earliest available point. Special care should be taken in requesting sensitive information, noting that individuals may feel more comfortable providing such information on an anonymous basis.

28. The Office submits that year of birth is an adequate indicator for statistical purposes, rather than date of birth as suggested in the Consultation Paper. Additionally, the Office submits that there should be a clear workforce planning need for each data item collected and it may be useful to consult on and publish this information.

Protection of unique identifiers

29. There are particular privacy risks around the use of unique identifiers which will need to be addressed. The Consultation Paper notes that unique identifiers enable the linkage and aggregation of disparate sources of information about individual practitioners. For this reason, many privacy laws restrict the adoption and use of identifiers that have been assigned to government agencies.

30. The Consultation Paper also 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 should also be consulted on the development of unique identifiers, including on any proposed safeguards to protect the use of identifiers.

Assessing risks and security measures for amalgamated databases

31. At present, collection and storage of practitioners' information occurs from disparate sources, namely the various registration and accreditation boards in each state and territory. The advent of the NRAS means that this information will be merged and it is therefore important to identify and minimise any accompanying risks that may arise.

32. Amalgamated databases are more likely to face increased pressure for secondary use proposals and can be more attractive targets for hacking and inappropriate data-mining.[9] These matters should be considered further as part of a PIA.

[9] 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.