ATTACHMENT A

Review of the Private Sector Provisions of the Privacy Act 1988

1. OVERVIEW

The Department of Health and Ageing (DOHA) has exposure to the *Privacy Act 1988*, both public and private sector provisions, on a range of issues, especially in the health information and health records related areas. This submission reflects the Department's experience with this broad range of issues.

2. There are three main aspects of the private sector provisions of the Privacy Act that have been identified as being an issue. One is the inconsistency in privacy regulation across Australia, including complaints and enforcement procedures, which has been identified as a particular problem for development of national e-health initiatives as well as in handling requests for information and other activities undertaken by the Department across jurisdictions and between public and private sectors.

3. Australian, State and Territory governments are investing in a number of e-health initiatives at the national level aimed at harnessing the potential of information management and information and communications technology (IM&ICT) to build a more effective and efficient health care system. A National E-Health Transition Authority (NEHTA) has been established by Health Ministers to progress critical national health IM&ICT priorities. The existence of different privacy arrangements has significant implications for much of the work to be undertaken by NEHTA.

4. A major focus of work in the e-health area for the Department is on implementing Australia's national electronic health records network, Health*Connect*, designed to overcome the gaps in information flow at the point of clinical care. While there is wide acceptance of the benefits that Health*Connect* can deliver, particularly in the areas of patient safety and quality of care, there is also recognition that there are privacy and security risks that need to be managed to ensure such benefits are realised. Personal health information is sensitive information, and both consumers and providers will need to have trust in how their information is handled within and external to Health*Connect* ahead of participating in this system. In this context, privacy and security issues are consistently identified as a key building block for Health*Connect* among all stakeholders.

5. Care is needed to ensure that individual privacy remains a key priority in the development of any new health information system. As personal health information becomes more widely dispersed and stored on larger database systems, it may potentially become more difficult for an individual to control the flow and exchange of personal information unless proper privacy safeguards are built in from the outset. Unless consumers and providers have confidence in the way that their personal health information is handled, they may well choose not to participate in such initiatives.

6. The co-existence of Commonwealth, state and territory health information privacy legislation has created a significant burden on private sector health care services in understanding and meeting respective obligations, as well as confusion for health consumers affected by dual legislative instruments.

7. The second issue concerns the application of provisions relating to contracted service providers and the standard clauses that have been developed for inclusion in contracts with the Department. In the context of the work of the Rural Health and Palliative Care Branch and in other areas of the Department, the private sector provisions of the Privacy Act primarily apply to contracted Commonwealth service providers in relation to their contractual activities. There are specific clauses in the standard funding agreements used by the Department that require contractors to adhere to the requirements of the Privacy Act and the Information Privacy Principles concerning the collection, storage, use and disclosure of personal information (i.e. disclosure of information and protection of personal information clauses).

8. The third issue concerns the use of information for purposes other than for which it was originally collected such as research in particular and some difficulties with the application of the Privacy Act.

2. BACKGROUND

9. Privacy is a fundamental principle underpinning quality health care. Without an assurance that personal health information will remain private, people may not seek the health care they need which may in turn increase the risks to their own health and the health

of others. Indeed consumers regard health information as different to other types of information and consider it to be deeply personal.[1]

10. Traditionally, health service providers have and continue to rely on the central notion of confidentiality, which acknowledges a person's right to be able to access a health service with an assurance that the health information he or she provides will not be disclosed to others. Because privacy protection is an integral part of quality health care, it is important that a strong and effective privacy framework is in place to regulate how and when individual's health information may be collected, stored and disclosed to others. The central focus of the framework should be on protecting individual's rights to have a choice about how their health information will be handled, so that ultimately individuals maintain some control over who has access to their health information.

11. The private sector provisions in the Privacy Act have made substantial inroads in creating a culture of privacy across the private health care sector, including the need to balance the individual's needs for privacy with the public's interest in having access to data for research and other secondary uses to benefit both individuals and their communities.

12. Health information is currently protected in a number of ways, ranging from common law to privacy legislation and the ethical and professional codes of practice that apply to most health service providers.

13. There are also a number of provisions in legislation, such as in Health Administration Acts and Public Health Acts that set out rules on how individual health information should be handled in certain situations.

[1] Consumer Attitudes Towards Consent, Electronic Health Records and the Use of Health Data for Research Purposes, TQA Market Research report. October 2004, DoHA

3. A SINGLE COMPREHENSIVE NATIONALLY CONSISTENT SCHEME

3.1 Inconsistency in current arrangements

14. The Department's experience indicates that the objective of establishing a single comprehensive national scheme provided through codes adopted by private sector organisations and the National Privacy Principles (NPPs) has not been met. Rather it is our experience that the private sector provisions now form just one of several layers of privacy requirements and legislation applying to the health sector, thus contributing to the complexity faced by both public and private sectors when addressing health privacy issues.

15. While the Privacy Act provides a platform for building a national privacy framework, the emergence of state privacy and health records legislation alongside the private sector provisions has created an increasingly complex set of arrangements and onus on private sector health professionals in understanding what their obligations are under the various regimes. This is likewise confusing for consumers who are unsure which legislation applies under what circumstances. For example, how they can access their own health record and what charges they should pay.

16. The end result is a patchwork of public and private sector legislation, common law and codes of conduct governing the handling of health information privacy in Australia, which in turn creates major problems for the future of national e-health initiatives such as Health*Connect*.

17. The need for consistent privacy arrangements across both the public and private sectors and jurisdictions has become even more pressing with these emerging developments in the management of electronic health records. Health service providers have an increasing capacity to gather, exchange and link health data about individuals on a larger scale than ever before. There are significant benefits arising from these developments, as not only do these technologies create opportunities to improve patient care but they can, at the same time, give consumers greater control over health care decisions that affect them.

18. The achievement of a viable and secure national health information network that facilitates the exchange of health information between and within health service providers – as proposed under Health*Connect* – requires a robust and consistent privacy framework. The greater use of telehealth in the future also raises issues of the need for consistency in privacy rules across jurisdictions, where service providers may be located in different states and territories.

19. The existing inconsistency in privacy regulation makes specific national projects such as Health*Connect* difficult to implement, as there is confusion about which principles apply and under what conditions. As a national network, Health*Connect* needs to have the same privacy rules in force across the private and public health sectors, and across all jurisdictions. This is particularly an issue in the health environment where individuals continually move between the private and public sectors and where providers will routinely deliver health care services in both sectors.

20. Under Health*Connect*, summary health information will follow the individual wherever and however they encounter health services. Information recorded in Health*Connect* will be then downloaded, subject to the individual's consent, into the health service provider's electronic system. While Health*Connect* can make its own national policy rules, it will be of critical importance that robust privacy arrangements are in place to protect the information once it resides in providers' systems – and that these arrangements can be consistently applied wherever the information resides.

21. In the absence of a consistent set of national rules, "the challenge for the implementation of Health*Connect* is to develop a single set of clear policies and procedures which complies with all relevant obligations and has universal application to all entities (whether public or private sector) and individuals in all Australian states and territories".[2]

22. The development of a national health privacy framework to achieve consistency for privacy arrangements across both the public and private sectors and jurisdictions has been supported by Health Ministers as a way to address the issue of differences that apply across jurisdictions and across public and private sector boundaries. The Privacy Working Group,

[2] Clayton Utz, Health*Connect* Legal Issues Report, November 2004

made up of Commonwealth, State and Territory representatives and established at the request of Health Ministers, developed a draft National Health Privacy Code which was released for public comment in early 2003.

23. The National Health Privacy Code is intended to provide a nationally consistent set of rules for the collection and handling of personal health information across the private and public health sectors. It takes into account the special needs of health both in protecting individual privacy and in facilitating communication between consumers and health professionals in the interests of good patient care. It also recognises that, if used wisely and with the utmost care, health information can be used in the public interest to build a better health care system. Essentially, the Code is about privacy and quality of care.

24. The main objects of the Code are:

"(a) to achieve national consistency in the handling of health information across the private and public sectors through the establishment of a single national code for the appropriate collection and handling of health information by public and private sector organisations; and

(b) to do so in a way that:

(i) ensures responsible and appropriate collection and handling of health information held in the public and private sectors;

(ii) achieves a balance between the public interest in protecting the privacy of health information with the public interest in the legitimate use of that information;

(iii) enhances the ability of individuals to be informed about their health, disability or aged care services;

(iv) promotes the provision of quality health, disability and aged care services; and

(v) engenders consumer and provider trust in the protection of health information privacy."[3]

25. The draft Code has been finalised by the Privacy Working Group and is to be considered by Health Ministers in 2005.

26. Departmental consultations with a number of stakeholders has also revealed that there is strong support for health specific privacy legislation - for example, the consultations relating to the proposed National Health Privacy Code and other consultations relating to the implementation of Health*Connect*.

27. Another marked change in the provision of health care services is the increasing difficulty in distinguishing between health services provided by private and public organisations. Many services are now co-located or are the result of a collaborative approach between public and private sector bodies. Not only is it difficult for consumers to understand what privacy standards apply in a given situation, it is sometimes difficult for health service providers to determine what privacy legislation they are bound by in a particular setting. The different privacy standards that currently exist in the public and private sectors have the potential to create a practical impediment to promoting more effective management of health information.

28. A recent example of the effect of several layers of privacy is a request for advice referred to the Department's Privacy Contact Officer. The issue concerned ACT pathologists changing their consumer forms (the changes have a privacy implication). To provide advice to ensure that the issue was fully covered required reference to:

- **Commonwealth Privacy Act 1988** which has coverage in the ACT for the public sector through the Information Privacy Principles (IPPs); coverage of the private sector NOT operating as a contractor for the ACT or Australian Government; and coverage of contracted service providers to Australian Government agencies;
- **ACT Health Records (Privacy and Access) Act 1997** which also covers the ACT private sector; and
- **Possibly other ACT Legislation** if the pathologist is operating as a private sector organisation.

3.2 Amendments to current legislation

3.2.1 Collection of family history

29. The collection of an individual's family history is an essential part of clinical care, as has been recognised by the Public Interest Determination made by the former Federal Privacy

[3] Draft National Health Privacy Code, http://www7.health.gov.au/pubs/pdf/code.pdf - page 3

Commissioner. The Department recommends that this capacity be included in the Privacy Act.

3.2.2 Deceased persons

30. The Act only applies to living persons. The Department supports inclusion of deceased persons who have been dead for 30 years or less within the scope of the Act, as proposed in the National Health Privacy Code.

3.3 Complaints

31. A significant element in the management of consumer complaints is the avenues available for consumers to seek redress. The avenues and processes open to consumers to ensure that their complaints are formally addressed need to be simple and easily accessible. However, privacy complaints mechanisms are inconsistent across jurisdictions, resulting in confusion for the health consumer.

32. Under current processes, where there is a complaint against a private sector organisation, the consumer can make a complaint to the Federal Privacy Commissioner or, in the case of Victoria and NSW, to a State Privacy Commissioner. For a complaint against a State or Territory public health sector organisation, the person can complain to the State/Territory health care complaints commissioner or the State/Territory privacy commissioner where one exists in that jurisdiction. In addition, other complaint or regulatory bodies such as health complaint commissioners, office of public advocates, professional registration boards (eg. pharmacy and medical boards) exist to address consumer complaints.

33. As an example, the Department receives requests, both by telephone and through Ministerial correspondence, from individuals for access to their medical records, as well as family member's medical records, both living and deceased. Recently, a request was received from an individual who had been refused access to medical records. Advice had originally been sought from the Office of the Federal Privacy Commissioner (OFPC), who, because of the complexity of the matter, had referred the matter to the Queensland Minister for Health for assistance. The Queensland Minister of Health had then referred the individual to this Department even though the Department had no jurisdiction in the matter. The matter was eventually referred to the Queensland Health Complaints Commissioner to address.

34. The unwieldiness of the arrangements for all participants as well as those responsible for managing day-to-day operations has been evident in the Health*Connect* trials and planned whole of state implementations. The apparent lack of clarity and definition relating to the recourse that consumers have when they feel that their privacy has been breached could also lead to significant confusion to vulnerable individuals in seeking remedies for their complaints.

35. The Department would prefer to see a more consumer-friendly approach for dealing with privacy complaints. One possibility could be for the OFPC to develop Memoranda of Understanding (MOUs) with Health Complaints Commissioners within jurisdictions to enable more complaints to be dealt with locally.

3.4 Penalties and Enforcement

36. The Department notes from data reported by the OFPC that complaints about health service providers are the second highest (14%) in industry sectors.

37. Given the highly sensitive nature of personal health information, and the potential for personal and social harm that can arise from misuse of such information, there is strong support among consumer and provider groups for penalties for breaches of privacy. This has been apparent in the consultations carried out in relation to Health*Connect* and Medi*Connect*, as well as those concerning the proposed National Health Privacy Code.

38. The OFPC should give serious consideration to the need for penalties to be imposed in relation to breaches of the NPPs for health information.

3.5 Provision of health services over the Internet

39. An area in which privacy concerns are raised is in the provision of health services over the Internet. It is apparent that the Internet is fulfilling a growing role in the provision of information and in some instances, treatment in the course of which a great deal of information, some which is ‘personal information' may be collected. The perception that privacy is protected is critical to the uptake and use of e-health services. The new technologies raise importance question in relation to the possible inappropriate use of data collected on information, prevention and consumer sites.

40. Health interventions delivered on line bring with them novel ethical and legal challenges. The use of sophisticated computer technology has facilitated the creation of sites that deliver personalised, tailored health interventions. These interventions seek to exploit the extraordinary capacity of the Internet to create a new way of delivering a health intervention and are characterised by their level of automation and interactivity. The degree of interactivity in the current generation of CBT sites is fairly limited, and thus their capacity to personalise the health intervention is correspondingly limited. However the capacity to effectively exploit interactivity will grow over time and as the sites become more sophisticated so to will the ethical and legal issues associated with them become more and more complex.

41. For many Australians the Internet has become a powerful and familiar health care tool. In *The Third Annual Australian e-Health Study*, a survey conducted by ACNeilsen and released in 2004, 5.6 million Australians aged 15 years and older who accessed the Internet were profiled. The survey found that 1.3 million use the Internet for 'health/medicines/information on conditions'[4].

42. As the Internet has become more sophisticated there has been a rapid increase in the number of e-health sites aimed at consumers, and in particular self help intervention sites. These sites deliver interventions designed to help people manage and improve their health through self-help. These initiatives do not facilitate direct contact between a health professional and consumer. Rather these self-help technologies involve systematically developed programs that provide interactive services to an individual. These sites typically seek to exploit the capacity of the Internet to personalise information to the particular consumer.

43. The designers of the sites ask for certain information, which if asked for in a face to face consultation with a health professional, would be considered a part of a health record. The information is used to enable the tailoring of information of relevance to the consumer. Importantly, these sites record all the information inputted by the consumer, which typically includes, for example, the scores of psychological tests.

[4] AC Neilsen Consult, the Third Annual Australian eHealth Study, 2004, DoHA

44. Under the Privacy Act, information only becomes personal information if the identity of the person providing the information "*identity is apparent, or can reasonably be ascertained, from the information or opinion*" (s 6). An obvious question that arises with this definition is at what point information about a person makes the transition to personal information. The reason this is important is because if information can be characterised as personal then it attracts the provisions of the Privacy Act. This question will arise in a number of circumstances but in particular in relation to email addresses that may be declared by individuals accessing online self-help intervention sites.

45. The move towards personalising health information is predicated on the assumption that targeted information is more effective at producing a measurable behaviour change than undifferentiated advice about a particular condition. However, it brings with it a new complexity for the creators of the site: are they merely giving generalised advice or are they offering a treatment to the user. The more health information is personalised and tailored to meet the needs of the individual "and the more it encourages the receiver to act upon the advice, the more we are moving within the continuum from giving general advice towards attempting to treat, and therefore practice medicine."[5]

46. If an intervention is characterised as 'treatment' rather than prevention information or promotion this will have certain legal and ethical implications for the site author: they may be characterised as a health service provider. While many online health transactions, in particular telemedicine, can be convincingly understood as replications of the transactions and relationships in the 'real' world, some cannot. This may have important implications for consumers: if they are receiving 'online treatment' through a fully automated CBT intervention are they entitled to the same legal rights and protection as a consumer receiving CBT in their GP surgery, including privacy rights? Alternatively the sites could be characterised as analogous to a self-help book and therefore attracting a lesser degree of legal protection? The answers to these questions will have important privacy implications.

[5] Eysebach G, towards ethical guidelines for dealing with unsolicited patient emails and giving teledvice in the absence of a pre-existing patient-physician relationship – systematic review and expert survey, Journal of Medical Internet research, 2002; 2(1)

47. The provision of teleadvice also raises jurisdictional issues about which privacy regulatory provisions apply. There is clear inconsistency for example between the Victorian legislation which is purported to cover the provision of information in respect of any resident of Victoria, where, if the teleadvice was provided from NSW, it might also be claimed to be subject to NSW legislation, as well as the Privacy Act. Where teleadvice is provided from outside Australia, it may not even be subject to any Australian privacy requirements.

4. CONTRACTOR PROVISIONS

4.1 Privacy Act application

48. Contractors with the Department have commented that they are obliged to comply with three sets of privacy principles: the National Privacy Principles (NPPs) which apply to them in their capacity as organisations; the Information Privacy Principles (IPPs) which are imposed on them, at least in part, as a result of the operation of section 95B of the Privacy Act; and the applicable State or Territory privacy laws.

49. It is conceded that the NPPs and the IPPs have many provisions in common so that compliance with one ensures compliance with the other. But there are differences and the combined regime is typically described as a "minefield".

50. That the provisions requiring Commonwealth contractors to abide by the IPPs and NPPs is complex and confusing is borne out by the Department's experiences in the Medi*Connect* Field Test where doctors and pharmacists were contracted to the Commonwealth. In addition to their existing privacy obligations under the Privacy Act, providers were required to comply with the Information Privacy Principles in respect of all personal information collected, used, disclosed or stored as part of the Medi*Connect* Field Test. To the extent that any existing obligations under the National Privacy Principles were inconsistent with the Information Privacy Principles, these were excluded during the conduct of the Medi*Connect* Field Test.

51. It has also been pointed out to the Department that Aboriginal Health organisations which receive funding from the Commonwealth and are not contracted service providers are nevertheless obliged to comply with the IPPs notwithstanding the fact that as private sector

organisations they are already bound by the NPPs. Examples of situations where the interaction between the IPPs and the NPPs is less than satisfactory follow.

52. Under the NPPs (eg NPP2) a Medical Service could liaise with immediate relatives in relation to the care of a patient. Hence, a GP can discuss the care of a person with another.

53. However, a different result arises where the Medical Service is funded under a Funding Agreement with the Commonwealth as are Aboriginal Medical Services. In the case of those services the standard clause in the Funding Agreement requires that the Service comply with the IPPs. In reality this means that the service has to comply with both the IPPS and the NPPs with the IPPs taking precedence where there is an inconsistency.

54. Hence a situation can arise where a patient is in attendance at a funded Medical Service and may be unable to communicate a consent regarding disclosure to a relative to the practitioner concerned.

55. In that case the IPPs are more stringent than the NPPs because the IPPs do not expressly deal with the issue of medical practitioners and the like communicating with relatives. Under the IPPs the disclosure would have to be necessary to prevent " a serious and imminent threat to life" in any case where the patient is unable to communicate consent.

56. The reality is that strict compliance with the IPPs by a funded Medical Service would mean that the relative could not be informed about the patient's condition and as a result patient care might well be compromised. It is an anomalous situation where a patient in a Medical Service received different treatment not for any medical reason but rather because of the method by which the Service itself is funded.

57. This is a clear case where compliance with the IPPs is inappropriate and the Service should be bound in the Funding Agreement to comply with the NPPs

58. In addition, a Medical Service funded by way of Medicare Payments under the Health Insurance Act, or a Medical Service funded by a State or Territory Government is not obliged to comply with the IPPs. Such a Service is obliged however to comply with the NPPs. In a

recent case an Aboriginal Medical Service (AMS) was funded by way of a tripartite agreement with a Territory Government. As a result the Commonwealth prepared Agreement required that the AMS comply with the IPPs. However, had the Commonwealth simply provided its contribution to the Territory Government and left the detailed arrangements with the AMS to the Territory Government the AMS would simply have been required to comply with the NPPs.

59. In other words, the question of whether the IPPs have to apply can in some cases be determined by the choice of funding method rather than by focus on the privacy needs in the particular case. The result is that there are medical services funded by the Commonwealth in the NT where the IPPs must apply. There is at least one community which is receiving medical services through the NT Department of Health as a result of the liquidation of the previously funded Organisation. The net result for that community is that while the Organisation was operating, the Funding Agreement required compliance with the IPPs and the NPPs applied. Now of course, the personal information about recipients of that service is only protected to the extent that the NT has privacy protections of its own in place. Neither the NPPs or the IPPs apply in that case.

60. In other cases it is foreseeable that the funding of a Medical Service by way of the provision of funds to the State / Territory Government for distribution would result in the application solely of the NPPs to that organisation.

61. It is remarkable that the patient's personal information may be given different protection, not because of any privacy considerations but rather because of the method of funding that the Commonwealth chooses to use.

62. The review process might therefore address the question of the practical effect of having IPPs imposed on private organisations that do not have contractual obligations to the Commonwealth and consider whether policy changes might be made.

63. In the Department’s view, it would be much simpler and more practical to require private sector contractors to abide by the NPPs.

5. SECONDARY USES OF DATA

5.1 Research use

64. The private sector provisions provide a good balance between protecting individual health information privacy while at the same time recognising that there are important public and individual benefits to be gained through secondary uses of personal health information such as for research.

65. From research conducted for the Department it is apparent that consumers have very definite opinions about health information. Generally they express strong reservations about the use of personal health information – that is identified information - being made available for any purposes other than their own clinical care. Consumers want to be informed about the information practices of their health service provider, however, importantly consumers are generally very accepting of the notion of sharing de-identified personal health information amongst health planners and researchers.[6]

66. The current provisions generally enable the flow of information between relevant health service providers in appropriate circumstances. However, there is anecdotal evidence suggesting that there is either a lack of understanding of appropriate secondary usage of information (ie. Where the secondary use is related to the primary purpose) or reluctance to use information for an appropriate secondary purpose. An example of this may be where a health fund has a range of health related information in relation to its members. An appropriate and reasonable secondary use of this information would be for the health fund to use the information to assist its members to manage their health (ie. Preventative programs). This would be of benefit both to the health fund and the member.

67. Notwithstanding the benefits, the coexistence of NHMRC Guidelines under Section 95 and Section 95A of the Privacy Act has created some confusion both for researchers and consumers. Since December 2001, a range of NHMRC stakeholders have expressed concern that implementation and/or interpretation of Commonwealth and State privacy legislation is compromising research and health care that would otherwise improve outcomes for both

individuals and public health. It has been suggested that this is an unintended effect of the privacy legislation and, more particularly, the private sector amendments to the Privacy Act.[7]

[6] Research Report 5: What will be necessary to manage privacy, ACNeilsen Consult, DoHA, 2003 p16; Consumer Attitudes Towards Consent, Electronic Health Records and the Use of Health Data for Research Purposes, TQA Market Research report. October 2004, DoHA

[7] Campbell Research and Consulting. *The Impact of Privacy Legislation on NHMRC Stakeholders* July 2004.