Australian Government

Office of the Privacy Commissioner

Consultation on the Australian Government Health and Social Services Access Card - Discussion Paper Number 2

Submission to the Department of Human Services: Access Card Consumer and Privacy Taskforce

March 2007

Table of Contents

Office of the Privacy Commissioner

1. 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, 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. On 21 February 2007, the Taskforce released *Discussion Paper Number 2: Optional Medical and Emergency Information (*'Discussion Paper 2'), and invited public comment.[1] This publication follows from *Discussion Paper Number 1*,[2] ('Discussion Paper 1') released on 16 June 2006, which canvassed a broad range of issues relating to the Department of Human Service's Access Card. In August 2006, the Office made its submission in response to Discussion Paper 1.[3]
3. The Taskforce states that the present Discussion Paper will form the basis for a protocol on the storage of personal medical information, with a view to introducing this protocol simultaneously with the Access Card registration process in April 2008.[4] The Office welcomes the opportunity to provide input into this process.
4. In addition to its engagement on Discussion Papers 1 and 2, the Office has also made the following submissions relating to the Access Card initiative:
    - Submission to the Office of Access Card regarding its *Consultation on the Exposure Draft of the Human Services (Enhanced Service Delivery) Bill 2007*;[5] and
    - Submission to the Senate Finance and Public Administration Committee Inquiry into the Human Services (Enhanced Service Delivery) Bill 2007.[6]

[1] Available at http://www.accesscard.gov.au/discussion/Discussion%20Paper%20Voluntary%20Medical%20and%20Emergency%20Information.pdf ('Discussion Paper'). Accessed 8 March 2007
[2] Available at http://www.accesscard.gov.au/discussion/060615_taskforce_discussion_paper.pdf. Accessed 8 March 2007
[3] Office of the Privacy Commissioner, Government Health and Social Services Access Card - Discussion Paper Number 1: Submission to the Department of Human Services: Access Card Consumer and Privacy Taskforce, p8. ('Access Card Submission No. 1'). Available at http://www.privacy.gov.au/publications/accesscard_sub_082006.pdf
[4] Discussion Paper, p 3
[5] Available at http://www.privacy.gov.au/publications/accesscardexposuresub.html.
[6] Available at http://www.privacy.gov.au/publications/sub-hsesd032007.html

5. The Office's recent submission in response to *Issues Paper 31* of the Australian Law Reform Commission Review of Privacy ('ALRC submission') also addresses issues relevant to the Access Card initiative. Chapter 11 ('Developing Technology')[7] and chapter 12 ('Unique Multi-Purpose Identifiers')[8] may be of particular interest in this area. The Office has also made a recent submission to the National E-Health Transition Authority (NEHTA) on NEHTA's *Privacy Blueprint – Unique Healthcare Identifiers*, Version 1.0, which may have relevant implications.[9]

Privacy Policy

Privacy Framework

6. In its previous submission to the Taskforce, the Office described a multifaceted approach which the Office believes is essential to a robust privacy framework.[10] Comprehensive privacy protection should be based on four elements, rather than attempting to rely excessively on a single tool.
7. These four elements can be expressed as:

Design + Technology + Legislation + Oversight

8. In brief, these elements can be explained as:
   - **System design**, including, card design, system architecture and the parameters governing what information is collected and what information flows are possible;
   - **Technological measures**, including, but not limited to, data security initiatives, as well as measures to minimise the degree to which existing systems become increasingly integrated, a consequence of which may be new and potentially privacy invasive flows of personal information;
   - **Legislative measures**, including defining the extent of the functions of the Access Card, proscribing purposes that fall outside those functions and introducing sanctions for misusing any aspect of the system or the personal information it handles; and
   - **Oversight mechanisms** that promote confidence in the system by assuring the community that the operation of the system is subject to stringent accountability measures, including provision for audit and independent complaint handling.
9. This submission will draw on this framework in responding to the issues raised by Discussion Paper 2.

Informing the community

[7] Available at http://www.privacy.gov.au/publications/submissions/alrc/c11.html
[8] Available at http://www.privacy.gov.au/publications/submissions/alrc/c12.html
[9] Available at http://www.privacy.gov.au/publications/sub-nehta-uhi-200703.pdf.
[10] Access Card Submission No. 1. Available at http://www.privacy.gov.au/publications/accesscard_sub_082006.html#mozTocId959788.

10. In the interests of transparency, the community should be fully informed about how their personal information will be handled as part of the facility for storing optional health information ('the facility'). A comprehensive communications strategy will help build community confidence, and encourage a greater number of individuals to take advantage of this voluntary feature.

11. In the Office's view, individuals must know what it is they are agreeing to if they decide to take advantage of the facility. As noted in the Office's *Guidelines on Privacy in the Private Health Sector* ('The Health Guidelines'),[11] for consent choices to be valid, they must be fully informed and freely given

12. In the present context, this would entail understanding the implications of the two-tier structure (if adopted), and what security protections apply to the information stored on the card. The individual should also be informed as to who they can approach if they have a complaint concerning the facility (see paragraph 65).

13. Consideration should be given as to where responsibility for implementing a communications strategy would lie, and how information would be disseminated. Questions for consideration include:

    - whether a media-campaign would be used, and
    - what role individual healthcare providers may take in providing the information.

14. The Office also notes that an Australian Government agency or private-sector organisation administering the Optional Medical Information component of the Access Card should consider its obligations under the Privacy Act to provide individuals with notice of how their personal information will be handled.

Risk-benefit analysis

15. The Office has previously noted the benefit of individuals being given appropriate choices regarding what information is stored on the Access Card, and emphasised the role of choice in sustaining community trust.[12] Voluntary Storage of Medical Information may provide an opportunity for individuals to exercise choices of this nature.

16. At the same time, the risks associated with such choices require careful consideration. Individuals should be fully aware of possible risks, including:

[11] Office of the Privacy Commissioner, Guidelines on Privacy in the Private Health Sector.' Available at http://www.privacy.gov.au/publications/hg_01.html.

[12] Access Card Submission No. 1, p 27. However, because of privacy risks, it may be inappropriate to provide individuals with the option of engaging in certain practices. One example of inappropriate provision for choice would be allowing individuals to consent to the use of the Access Card number as an identifier when dealing with private sector organizations.

- the potential for inappropriate disclosure of information (see discussion beginning at paragraph 32); and
- the potential for the information to be inaccurate and hence, unreliable in an emergency (see discussion beginning at paragraph 44).

17. Discussion Paper 2 notes the 'overwhelming weight of submissions' to the Taskforce's first enquiry in support of storing optional medical information.[13] The Office submits, however, that while such a facility has broad in-principle support, the details of how such options are exercised will be crucial.

Issues raised in recommendations

Storage structure

Taskforce Recommendation 1: That the Taskforce's preferred two-tier model be considered as a standard should the inclusion of voluntary emergency and health information be available to the individual for inclusion on their Access Card chip.

Tier 1 information

18. The Office supports a two-tier model in principle. However, it appears that details of such a model would benefit from further consideration to ensure that the model is privacy-enhancing, rather than potentially privacy-invasive.

19. Discussion Paper 2 states that the first tier of the system would contain only information that is absolutely necessary to enable provision of emergency health treatment. This information would be 'accessible to anyone with an approved reader.'[14] Particular types of information collected for storage in this area are discussed below at paragraph 41. For present purposes, it is sufficient to note that information stored may include health information, such as allergies.

20. The Office is concerned by the statement that optional medical information is 'in the public domain.'[15] The Office suggests that the exact implications of this expression could be usefully clarified. For example, under the Privacy Act, while generally available publications are exempt from regulation, personal information contained within such sources may still be afforded privacy protections. The Office has prepared an Information Sheet on this matter.[16]

[13] Discussion Paper, p 4
[14] Discussion Paper, p 5
[15] Discussion Paper, p 6
[16] See Information Sheet 17 *Privacy and Personal Information that is Publicly Available* available at http://www.privacy.gov.au/publications/is17_03.html.

21. Privacy safeguards may be incorporated into the facility's design by implementing dedicated card-readers. A system of this kind may ensure that only authorised readers would be able to access emergency health information (see discussion beginning at paragraph 38).

22. Alternatively, if the present security arrangements around Tier 1 information are retained, individuals should be adequately informed about the privacy risks, including the possibility that their optional medical information may be accessed in non-health contexts.

Current legislative framework

23. NPP 10.1(c) provides that, where there may be a serious and imminent threat to the life or health of any person, a health service provider may collect the information necessary to lessen or remove the threat, without having to obtain the individual's consent. Consideration of this provision may be found in the Office's ALRC submission.[17]

24. Personal information collected in emergency situations pursuant to NPP 10.1(c) is not, in effect, released into 'the public domain.' Accordingly, such collection of sensitive health information for use in an emergency does not affect the level of protections which would otherwise apply to how this information is subsequently collected, or used and disclosed. The Office submits that NPP 10.1(c) both enables necessary access to health information in an emergency, and ensures that privacy protections remain.

25. Accordingly, the Office submits that the policy settings established by NPP 10.1(c) should inform subsequent policy development, in preference to the notion of information being 'in the public domain', which might suggest that such information is not afforded privacy protections.

26. In addition, the Office notes that NPP 10 will proscribe the collection (as opposed to the mere 'viewing') of health information by organisations except where permitted by a relevant exception. The Office would be concerned, for example, if health information were 'incidentally' collected when an Access Card is read for another purpose, such as to validate an entitlement. Guidance material may assist in highlighting this issue to organisations.

27. The Office also notes that the proscription established by NPP 10 against the collection (whether intentionally or accidentally) of health information, would not apply to Access Card users that fall outside of the Privacy Act's jurisdiction (such as many small businesses and state government bodies). Accordingly, such a prohibition could usefully be adopted in legislation accompanying the Access Card.

Tier 2 information

28. Discussion Paper 2 states that the second tier would contain PIN-protected health and medical information. Access to this information would be controlled by the individual cardholder.[18]

[17] Available at http://www.privacy.gov.au/publications/submissions/alrc/c8.html#Collection3
[18] Discussion Paper, p 5

29. Discussion Paper 2 also emphasises the separation between the Access Card initiative, and the Shared Electronic Health Record agenda (SEHR).[19] The National E-Health Transition Authority (NEHTA) states that SEHRs:

> 'Will enable authorised healthcare professionals to access an individual's healthcare history, directly sourced from clinical information such as test results, prescriptions and clinician notes.'[20]

30. Discussion on this issue may be assisted by a clearer indication of the difference in scope between the two initiatives. It is unclear, for example, whether the Access Card would only store discrete items of medical information (such as 'suffers haemophilia'), as opposed to the SEHR, which may store comprehensive treatment information.

31. Discussion Paper 2 does not explicitly state what information would be stored in Tier 2, but notes that any such information would be collected in accordance with the remainder of the paper's recommendations.[21] Discussion on this point would be assisted by an indication as to what information is envisaged as being stored in this tier.

Security

32. Robust technological security measures are one element of a comprehensive privacy framework (see paragraph 8). Such measures are necessary both to mitigate privacy risks, such as inappropriate access to personal information, and to build community trust in the initiative. Individuals are more likely to take advantage of an optional feature (such as storing medical information) where they have confidence that their personal information will be adequately protected.

33. On this basis, the Office suggests that allowing open access to emergency information (including, potentially, to non-emergency service providers and organisations) may not confer security protections that accord with community expectations.

34. The Government envisages Access Cards being used in an array of contexts, in both the public and private sectors.[22] As noted above the Taskforce's model envisages information stored in Tier 1 as being accessible to anyone with an approved reader.[23]

35. Because of the Access Card's wide range of potential applications, unrestricted access to emergency information may allow this information to be accessed unnecessarily. For example, an entitlement agency officer who swipes an individual's Access Card to verify their entitlement to

[19] Discussion Paper, p 9
[20] National E-Health Transition Authority, 'Shared Electronic Health Records.' Available at http://www.nehta.gov.au/index.php?option=com_docman&task=cat_view&gid=130&Itemid=139. Accessed 8 March 2007
[21] Discussion Paper, p 5
[22] The former Hon Joe Hockey MP, 'Future Directions for the Access Card: Your Card, Your Security.' Speech to National Press Club, Canberra, on 8 November 2006 http://www.accesscard.gov.au/speeches/press_club_speech_081106.pdf at p9. Accessed 8 March 2007
[23] Discussion Paper, p 5

benefits may be able to view information about the individual's allergies or chronic illnesses. Discussion Paper 2 notes this risk.[24]

36. The Office submits that the Access Card system should be designed in such a way that the information is only accessible where necessary to lessen or prevent a threat to individuals' life, health or safety.

Technology solutions

37. The issue then arises as to how the facility may be designed to ensure that information is only viewed where necessary. Discussion Paper 2 notes the difficulties associated with PIN protections:

    a. Because this form of authentication is controlled by the individual, it would be ineffective in situations where the individual is unable to communicate consent;[25] and

    b. Releasing readers capable of overriding PIN-protections poses security risks for other information which may be stored on the card.[26]

38. However, alternative technological approaches may provide security protections while avoiding the difficulties attending PIN-based access. Specifically, it may be possible to allocate a particular portion of the user-controlled space on the Access Card chip for emergency information, and implement specific security protections around this area. For example, access restrictions around this section could ensure that only a specially-designed reader would be able to access the information. The availability of these readers may then be limited to emergency service personnel, with this limitation being supported by legislative measures.

39. This alternative approach does not provide an absolute guarantee of security. It could be possible, for instance, for a person to gain unauthorised access to one of the readers. The benefit of the alternative approach is that the consequences of such a security breach are relatively contained. The unauthorised person would only access emergency medical information, as opposed to all PIN-protected information.

40. The Office suggests that further consideration be given to this, and any other technological approaches that the Taskforce may encounter, to ensure that adequate security protections are in place around the facility.

Information to be stored on the card

Taskforce Recommendation 2: That consultations be undertaken with the relevant medical and emergency service authorities to draw up an agreed definition of what should be regarded as 'absolutely necessary' medical data to be included in the first tier of the proposed model.

[24] Discussion Paper, p 13
[25] Discussion Paper, p 6
[26] Discussion Paper, p 6

41. Discussion Paper 2 emphasises that whether collecting a given piece of information is 'absolutely necessary' should be determined by reference to a clearly defined purpose. This principle is reflected in the threshold question posed in the paper:

> 'What information is absolutely necessary to be available from the Access Card chip to facilitate emergency medical treatment of a person in a crisis situation…'[27]

42. The Office supports Recommendation 2. The following comments relate to specific items of information which Discussion Paper 2 suggests may be included.

Medical conditions

43. Discussion Paper 2 recognises the stigma associated with certain conditions (for example, HIV or Hepatitis C status) and states that the Access Card should not store indications of these conditions.[28] The Office supports the Taskforce's position on this matter.

44. The Office also notes potential sensitivities surrounding other medical conditions. Discussion Paper 2 lists epilepsy, asthma, diabetes, haemophilia and allergies as conditions which may be recorded on the Access Card. Conditions such as these may not necessarily create the same scope for discrimination as conditions such as HIV status. Nevertheless, individuals may regard such conditions as highly personal information. The need to respect such sensitivities is reflected in the Privacy Act's National Privacy Principles, which afford a higher level of protections to all health information.

45. Accordingly, the Office submits that each condition suggested for inclusion be closely examined to ascertain whether recording them is indeed absolutely necessary for providing emergency healthcare. In particular, evidence would be required that recording such items on the Access Card would confer a definite and immediate advantage on emergency service personnel, compared to current diagnostic tools and practices.

[27] Discussion Paper, p 4
[28] Discussion Paper, p 6

Medications

46. Discussion Paper 2 notes that details of some medications could be stored on the Access Card,[29] particularly where they may have life threatening implications for the individual. However, NEHTA has also raised prescription information as a possible item for inclusion in a SEHR.[30] As this information would be Tier 1 data, it would be essential that individuals are provided clear information about the degree to which it may be accessible by others. This would especially be the case where a particular medication may disclose, either directly or by implication, an underlying medical condition.

Mechanism for managing individual choice

47. The Office understands that the consultation process under Recommendation 2 will result in a closed list of information which is eligible for voluntary storage. All other items would be excluded.

48. The Office would welcome further information regarding how the boundaries of this list would be enforced. Possible measures include:

- legislation specifying what information may be collected, and proscribe the inclusion of other items; and
- designing the data-entry process such that only specified types of data can be entered.

49. These, and other possibilities, could usefully be explored as this aspect of the Access Card progresses.

Verifying optional medical information

Taskforce Recommendation 3: That no Optional Medical information be entered into any part of the Access Card without verification of the accuracy of that information by an approved medical or other practitioner.

50. The Office understands that the policy objective behind Recommendation 3 is to ensure that information entered on the card is of sufficient integrity to be relied upon in an emergency.

51. Discussion Paper 1 raised concerns regarding the accuracy and currency of optional health information.[31] The Office's previous submission noted that the utility of the system can be compromised where the individual has

[29] Discussion Paper, p 5

[30] National E-Health Transition Authority, Shared Electronic Health Records. Available at http://www.nehta.gov.au/index.php?option=com_docman&task=cat_view&gid=130&Itemid=139. Accessed 8 March 2007

[31] Access Card Consumer and Privacy Taskforce, Discussion Paper Number 1 at p 26. Available at http://www.accesscard.gov.au/discussion/060615_taskforce_discussion_paper.pdf at p26. Accessed 8 March 2007

failed to keep their health information (for example, allergy notifications) up-to-date.[32]

52. To address this issue, the Taskforce proposes a system requiring that information is verified by an authorised professional before it is entered into the chip.[33]

53. The verification process provides a degree of certainty that the information was accurate at the time it was last updated. However, aspects of an individual's medical condition may change more rapidly than the updating process can capture. For example, if the section stores a notification of prescribed medication, the information may become inaccurate where the individual stops taking that medication, and delays arranging for the information to be updated.

54. For this reason, consideration should be given to limiting the scope of optional medical information to be stored to information which is reasonably static, or where the consequences of that information being out-of-date are not severe.

55. The Office also notes that, given the optional nature of the facility, the Access Card is unable to serve as a conclusive indicator of whether an individual suffers a given condition. Accordingly, it is unclear whether, in an emergency situation, a medical professional would regard an absence of allergy information as indicating a negative result, or simply an incomplete record.

56. This issue may be usefully addressed as part of educating health service providers in the use of the facility.

Accuracy of a printed symbol

57. The Taskforce suggests that a symbol may be printed on the face of the card to indicate that optional health information is stored on the chip.[34] The Office has concerns about the utility of this symbol, given that the Access Card is likely to have a lifespan of several years.[35] Given the possibility of change in the individual's condition over this time (or that the individual may simply decide they no longer wish to use the facility and arrange for their stored information to be deleted), a printed symbol may provide emergency services personnel with misleading information (including where providers incorrectly assume that the absence of a symbol infers that there are no allergies or so on).

58. The Office suggests that individuals should be fully informed as to the risk of inaccuracy associated with the use of a printed symbol if their condition changes.

---

[32] Access Card Submission No. 1. Available at http://www.privacy.gov.au/publications/accesscard_sub_082006.html#mozTocId279739

[33] Discussion Paper, p 8

[34] Discussion Paper, p 5.

[35] On 9 May 2006, a Media Release from the Hon Joe Hockey MP (then Minister for Human Services) stated that Access Cards would be replaced approximately every seven years. http://www.accesscard.gov.au/media/access_card_to_cut_red_tape.html. Accessed 8 March 2007.

Individual control

59. The Office notes that Recommendation 3 is likely to promote data quality and accuracy.

60. The Office suggests that there may be value in further considering what procedure would exist for removing information from the card. For example, if a person makes an informed decision to cease taking medication, it is not clear whether the person would need to have an authorised person remove this information on their behalf, or what fees may apply.

61. The Office would be concerned if an individual's capacity to alter their card information was restricted in this way. As the Office advocated in its previous submission to the Taskforce, individuals should have control over how their personal information is handled, afforded by offering a range of informed choices that are accessible and freely exercised.[36]

Legislative framework

Taskforce Recommendation 4: That the medico-legal issues arising from persons acting in good faith on the medical data contained in an Access Card be addressed and clarified in future legislation related to the operation of the Access Card chip.

Medico-legal issues

62. The Office notes the above recommendation. At this point, the Office does not have substantive comments, but would welcome being kept informed of subsequent developments.

Project-specific privacy legislation

63. In addition to medico-legal issues, the future legislation referred to in Recommendation 4 offers an opportunity to set essential parameters around how the individual-controlled area of the card is designed and implemented.

64. The Office supports Discussion Paper 2's statement that effective sanctions should be available and applied to people or organisations who interfere with an individual's privacy in relation to this information.[37]

65. Features of an effective legislative scheme were discussed in the Office's previous submission to the Taskforce. In brief, they consist of:

- Clearly defined complaint-handling mechanism
- Sanctions and remedies for inappropriate access, use and disclosure of the information

[36] Access Card Submission No. 1. Available at http://www.privacy.gov.au/publications/accesscard_sub_082006.html#mozTocId596873.
[37] Discussion Paper, p 6

- Powers of audit and investigation for the relevant oversight body and
- Provisions addressing the question of jurisdiction to ensure national coverage.[38]

66. Further discussion on auditing disclosures of health information may be found in the Office's ALRC submission.[39]

Broader legislative policy

67. Voluntary storage of medical information is one of the issues which may be addressed by future legislation. This issue also presents an opportunity to consider broader questions concerning the individual-controlled area of the Access Card.

68. This issue was addressed in the Office's recent submission to the Senate Finance and Public Administration Committee concerning the *Human Services (Enhanced Service Delivery) Bill 2007* which addressed the above issue. In this submission, the Office noted:

> 'In the interests of data integrity and security, consideration should be given (possibly in future legislation) to dealing with the risk of viruses, 'spyware' and other inappropriate software being stored on the chip, with the intent of modifying any person's card or interfering with the Access Card system.'[40]

69. Accordingly, consideration should be given to introducing comprehensive privacy safeguards around the user-controlled area of the chip.

Shared electronic health records

Taskforce Recommendation 5: The Australian Government, in its information campaign, restate its policy that the Access Card will not be used to store electronic health records or link to existing electronic health records.

70. The Office supports Recommendation 5. The Office also notes the Office of Access Card's statement that health records will not be stored on the smartcard, in the chip, or be held by the registration service.[41]

71. As noted at paragraph 30, the Office suggests that subsequent policy documents in this area could make a clear distinction between discrete items of health information, such as an allergy notification, and treatment

[38] Access Card Submission No 1. Available at http://www.privacy.gov.au/publications/accesscard_sub_082006.html#mozTocId514438.
[39] Available at http://www.privacy.gov.au/publications/submissions/alrc/c8.html#Noting
[40] See paragraph 41 of the Office's submission to the the Senate Finance and Public Administration Committee concerning the Human Services (Enhanced Service Delivery) Bill 2007 Available at http://www.privacy.gov.au/publications/sub-hsesd032007.html
[41] Office of Access Card, About the Card. Available at http://www.accesscard.gov.au/about_card.html. Accessed 8 March 2007.

notes, the latter of which the Office understands are intended to be the province of Shared Electronic Health Records.[42]

72. Particular privacy issues associated with electronic health records are addressed in the Office's ALRC submission.[43]

Interactions with third parties

73. This section of the Office's submission addresses issues of how the user-controlled portion of the Access Card chip may enable communications with third parties, either by linking to external databases, or recording other individuals' contact details.

Taskforce Recommendation 6: At the point of registration, card applicants could be given the chance to give informed consent to some flagging in either or both of the customer controlled section of the chip, or the register itself to any record which is be held in relation to their organ donor status by Medicare Australia.

Consistency between optional data linkage and the two-tier framework

74. The Office notes that Discussion Paper 2 considers the possibility of "flagging" relationships between the Access Card and other medical information systems, including for purposes other than providing emergency health care to the individual. The proposed linkage to Medicare Australia's organ donor registry is one example of such a linkage.

75. The Office notes that such a flag would not appear to fall within the definition of a Tier 1 data item. At the same time, if the flag, such as that indicating organ donor status, were stored in the PIN-protected Tier 2, then it is unclear how it would be accessed if the individual was incapable of providing the PIN.

76. The Office suggests that further consideration be given as to how the policy settings around the two-tier framework may accommodate such flagging.

77. More generally, the Office has some concerns about what is envisaged by the use of the term "data linkage" in this context. It is unclear whether the Access Card would merely contain a flag indicating that data is held in another source about that individual, or whether there would be some active data linkage between the two. The latter would seem to allow scope

[42] National E-Health Transition Authority, Shared Electronic Health Records. Available at http://www.nehta.gov.au/index.php?option=com_docman&task=cat_view&gid=130&Itemid=139. Accessed 8 March 2007.

[43] Available at http://www.privacy.gov.au/publications/submissions/alrc/c8.html#L20635

for an incremental expansion in functions of the Access Card and may raise the privacy risk of "function creep."[44]

MedicAlert information

Taskforce Recommendation 7: That direct linkages between the Access Card customer controlled part of the chip and services which provide direct assistance or instruction about the provision of emergency medical services (such as advanced directives or Medic Alert-type schemes) be accepted as the customer's choice and control, in terms of usage of the Access Card.

78. The MedicAlert website describes the system as comprising:
    - a metal token, with a logo on one side, and emergency medical information on the other;
    - a confidential national registry, storing: medications, emergency names and contact numbers of doctor, next of kin, etc. plus any other information which should be known in an emergency;
    - a 24 hr hotline; and
    - a Membership card, storing: information held on the national registry, as well as the phone number of the hotline.[45]
79. The Office suggests that the case for voluntary linking from the Access Card to MedicAlert's systems could be framed more clearly.
80. The Office also notes MedicAlert's first submission to the Taskforce, which expresses concern at the utility of storing emergency medical information on the Access Card chip, and in particular, MedicAlert's request that the Taskforce endeavour to 'have the emergency health details excluded from the Card.'[46]
81. Without further detail, the Office would have some unease about the general policy of creating linkages between the Access Card and other databases unrelated to the provision of government benefits. In particular, such a facility should only be undertaken where protections are in place to limit the creation of future additional linkages, including for purposes that may become increasingly remote from the original stated functions of the Access Card.
82. Given these concerns, the Office would be unlikely to support linking MedicAlert's systems with the Access Card.

[44] 'Access Card Submission No. 1' defines function creep as 'the process of incremental expansion in the purpose for which a system or object is used, to the point that it is employed for purposes that were not initially agreed to or envisaged.' See http://www.privacy.gov.au/publications/accesscard_sub_082006.html#mozTocId656684

[45] Australian MedicAlert Foundation. http://www.medicalert.com.au. Accessed 8 March 2007.

[46] Australian MedicAlert Foundation, 'Submission to Consumer and Privacy Taskforce Discussion Paper No. 1.' Available at http://www.accesscard.gov.au/discussion/1S4_australia_medic_alert_foundation.pdf. Accessed 8 March 2007.

Advance directives and third party contacts

83. Advance directives (or 'living wills') typically contain instructions left by an individual about their preferences regarding what medical treatment is administered or withheld in the event that they are unable to communicate consent.[47]

84. However, as discussed above (see paragraphs 77and 81), it is unclear the extent to which such functionality, once enabled, would permit for future linkages between the Access Card and third-party datasources. The Office is concerned that enabling linkages to third-party databases would allow scope for function creep. .

85. In regard to recording third party contact details on the chip, the Office agrees with Discussion Paper 2 that such a practice may raise privacy issues if a third party is not consulted by the individual. This issue could be addressed by administrative measures, such as by providing notice to the Access Card holder that they should seek the consent of an individual before recording their details. The Office notes that such a measure may not offer recourse to the third-party individual if their consent is not obtained. Accordingly, it may be necessary to consider whether the potential benefits and risks of such a facility can be reconciled.

The role of the Privacy Commissioner

Taskforce Recommendation 8: That the Office of the Privacy Commissioner be actively engaged in any development of policy in relation to the Optional Medical and emergency information.

86. The Office supports this recommendation.

Governance and oversight

Taskforce Recommendation 9: Once decisions about the inclusion of medical and health data have been made, the Australian Government must consider the question of whether such a scheme should be administered in the public sector or by some private sector operator chosen in an open tender process.

87. The discussion preceding Recommendation 9 focuses largely on the arrangements for inputting data onto the user-controlled portion of the card. It is unclear where oversight of the facility would lie, or the proposed

[47] NSW Young Lawyers, 'Older People and the Law: Chapter 2 – Taking Control of Your Health Decisions.' Available at http://www.lawsociety.com.au/page.asp?partid=7000. Accessed 8 March 2007.

nature of Government involvement beyond setting technical protocols for entering Tier 1 information. Discussion Paper 2 considers whether:

> 'Some hybrid arrangement could be appropriate, namely that the Government would approve the standard by which information would be entered into the Tier 1 section of the chip (the entry of data being by approved practitioners using their own systems) whereas any other arrangements for data entry below Tier 1 level could be managed/operated by others.'[48]

88. Regardless of how the system is managed, the Office would expect the necessary level of privacy protections to be met. Accordingly, the Office submits that future legislation should set out oversight functions for the facility.

89. However, the Office is not opposed in principle to data entry being managed through private-sector organisations, should the facility be implemented, and looks forward to productive engagement with the sector on this issue.

Other privacy issues

Children and impaired consent

90. Discussion Paper 2 gives a general overview of issues associated with children and the Access Card.[49]

91. For a proportion of Access-Card holders, their decision-making ability will be affected by factors other than an emergency medical situation. These individuals may still benefit from the optional medical information facility, should it be implemented. For example:

- a person with a intellectual disability may also have an allergy to certain medications or
- if a child has a separate Access Card, some information may need to be added, for example, parents' contact details and other emergency medical information.

92. These individuals may require an authorised representative to assist them in recording optional medical information. In particular, consideration may be given to how a representative's authority to act on the individual's behalf may be appropriately verified. Further discussion on appropriate verification in these circumstances may be found in the Office's ALRC Submission.[50]

93. The Office's ALRC submission also gave consideration to broader policy issues surrounding impaired consent. Key issues raised in this submission were:

[48] Discussion Paper, p 13
[49] Discussion Paper, p 12
[50] Available at http://www.privacy.gov.au/publications/submissions/alrc/c8.html#Representa

- There is considerable variation in the degree to which children or persons suffering impaired decision-making ability are able to make decisions on how their personal information is to be handled.
- Individuals may lack full capacity, but retain the capacity to exercise consent to a certain degree, or in certain cases. Individuals should be supported in making these choices to the fullest extent possible.
- The interests of the individual should be the primary consideration.[51]

94. The Office suggests that these issues be factored into ongoing policy development.

Privacy impact assessment

95. The Office's first submission to the Taskforce noted that the Access Card initiative could benefit from Privacy Impact Assessments (PIAs) being conducted at key points during its development.[52] The facility for storing optional medical information is a further instance where a PIA may be helpful in addressing privacy issues and offering solutions to address such matters.

[51] ALRC Submission. Available at http://www.privacy.gov.au/publications/submissions/alrc/c9.html#L23305.

[52] A Privacy Impact Assessment (PIA) is an assessment tool that describes in detail the personal information flows in a project, and analyses the possible privacy impacts of the project. Further information on Privacy Impact Assessments is available from the Office's publication, Privacy Impact Assessment Guide (available at http://www.privacy.gov.au/publications/PIA06.pdf).