Australian
Privacy
Foundation

post: GPO Box 1196
Sydney NSW 2001

email: noIDcard@privacy.org.au

web: www.privacy.org.au

22 March 2007

Access Card: Inclusion of voluntary medical and emergency information

Australian Privacy Foundation's submission in response to Taskforce Discussion Paper No. 2

Executive Summary

As noted in our submission to the Taskforce's Discussion Paper No. 1, the Australian Privacy Foundation (APF) opposes the proposed Access Card, and does not accept that it should proceed.

The APF does not oppose specific balanced proposals to meet important objectives in the areas of social security benefits administration and, separately, health benefits administration.

Nor does the APF oppose sensible proposals to improve access to necessary, life-saving medical information in medical emergency situations.

However we believe that it is not the objective of the Access Card to deliver medical information in medical emergency situations; nor do we believe that the Access Card's design allows for the best mechanism to deliver medical information in medical emergency situations.

We also believe that incorporation of this feature into the Access Card is an example of function creep, and opens the door for yet more function creep. The privacy implications of inclusion of data on the Register has also been completely overlooked.

We therefore recommend:

- that this feature be dropped from the Access Card proposal entirely
- that the Government instead help promote existing systems such as Medic Alert, both for potential clients and to explain how these systems should be used by members of the public in first aid situations
- that the results of the Taskforce's research and consultations on this feature be provided to NEHTA

CONTENTS

About the Australian Privacy Foundation

The Australian Privacy Foundation is the leading non-governmental organisation dedicated to protecting the privacy rights of Australians. We aim to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

Since 1987 the Australian Privacy Foundation has led the defence of the rights of individuals to control their personal information and to be free of excessive intrusions. We use the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed.

For further information about us see www.privacy.org.au

Lack of consultation about this aspect of the proposal

We wish to start by expressing our frustration with the so-called consultation process followed in relation to this aspect of the Access Card proposal.

The Taskforce's Discussion Paper (at p.3) refers to a Background Information Paper circulated in December 2006. We have no knowledge of that paper, and we cannot find it on the Taskforce's website.

While we were indeed invited to a "round table panel" on 15 December 2006, the invitation was only issued at short notice, and the date of the event – the week before Christmas, notoriously busy with end-of-year commitments – was so ludicrously inconvenient that our Campaign Director was unable to attend. Our Chair was available on that date, but in the absence of paid travel expenses, was also unable to attend.

We submit that a non-published paper, and a single event immediately before Christmas, organised at short notice and without provision for expenses of attendance to be reimbursed, does not make a "consultation process". We also note that no minutes or outcomes of that roundtable panel – or even attendance lists – have been published.

We therefore question the assertion (at p.3) that "representatives of all areas" attended the "major round table panel" on 15 December 2006.

As a result we also question assertions arising from that event.

In particular, the Taskforce's Discussion Paper begins by stating that:

> "The overwhelming weight of submissions made to the Taskforce gives strong support to the principle that emergency health and medical data should be included in the customer controlled area of the access card" (p.4).

We ask: what submissions is the Taskforce referring to?

As far as we knew, this Discussion Paper presents the first call for submissions on the topic of the inclusion of emergency health and medical data on the Access Card.

Back to first principles – feature is unrelated to project objectives

The Taskforce's Discussion Paper describes as the "threshold question": "what information is absolutely necessary (to be held on) the access card?"

We submit that this is not the threshold question. The Taskforce has skipped asking more fundamental questions about whether this feature should exist at all.

The *real* threshold question is:

> ***Why should there be any medical information on the Access Card <u>at all</u>?***

In other words:

> ***How does this feature relate to the objectives of the Access Card?***

The second Minister in charge of the Access Card, Senator Ian Campbell, recently suggested that he would drop this feature of the Access Card proposal entirely, as it was superfluous and troublesome.

We agree.

The communication of necessary, life-saving medical information in medical emergency situations has nothing whatsoever to do with the twin aims of the Access Card:

- to improve people's access to government benefits (health and social services) payments, and
- to reduce benefits fraud.

This feature is unnecessary

In our submission to Discussion Paper No. 1 (see Appendix B), we asked the Taskforce the specific question:

> ***What research has been done into the efficacy or utility of storing this information on a chip inside a 'secure' card which needs a reader to access it, as opposed to say a laminated piece of paper kept in one's wallet?***

Our question remains unanswered.

Further questions that should be asked of this proposal are:

> ***What is the most effective way to communicate medical information in an emergency?***
>
> ***What is the least privacy-invasive way to communicate medical information in an emergency?***

The Taskforce's Discussion Paper notes numerous problems with using the Access Card to communicate medical information to third parties, for use in emergency situations.

It is not clear what sort of 'emergency' would be better managed by information on an Access Card. The card-holder, presumably, would have to be unable to communicate the information. The person attending must have an authorised Access Card reader, so its no use if someone gets seriously sick or injured in any circumstance where rescue depends on an off-duty health professional, or a passer-by rendering first aid.

The person must also be able to link the person with a card. If two women are in the same car in a car crash, which handbag holds the wallet with the right card in it and how much time do you spend looking? If a person is rescued from a shark attack, what obligation will there be to find their belongings on the beach and check their ID card before taking them to hospital? Unlike the other tokens that are used, ID cards are not always carried on the person. We understand that ambulance officers and other emergency personnel are trained to assess the health and injuries of a person by observation and act quickly to respond to the situation as they perceive it. Hesitating to act while looking for information on a card that they may not find is contrary to their training and compromises the quality of care. If the person is able to tell the health professional where their card is during an emergency, they are able to tell you them the vital medical information that they need to know.

The Taskforce's Discussion Paper itself refers to the existing Medic Alert system, which "addresses all of the questions raised above about health status verification and the listing of emergency contact details" (p.10).

We therefore submit that the Taskforce should ask further questions:

> ***What is wrong with the existing systems, such as Medic Alert, used now?***
>
> ***How would the Access Card make any improvement compared to existing systems?***

In the absence of some evidence that there is anything wrong with the systems being used now – other than, perhaps, the fact that they may not be as well-known to the majority of Australians as it should be – we submit that there is no case to duplicate or replace existing systems such as Medic Alert.

We submit that the Medic Alert system of bracelets, pendants and badges, which are clearly visible, easily accessible in an emergency, and require no technology to use, and which protect privacy more so than a card would, is both a more effective, and less privacy-invasive, way to communicate medical information than the Access Card.

We suspect that this feature of the Access Card was proposed by or to the first Minister, Joe Hockey, by someone completely ignorant of existing systems.

This feature smacks of being an application dreamt up in a policy vacuum, to shore up support for the otherwise-unpalatable Access Card.

This feature is complex

We also note that while this feature may sound like 'common sense', it is, as the Taskforce readily acknowledges, far more complex than first thought. Even developing a uniform 'language' for written medical information is a mammoth task. The Taskforce has not even yet proposed what medical data might be necessary for inclusion.

We note that the National E-Health Transition Authority (NEHTA) is already tasked with developing the necessary tools and infrastructure to facilitate electronic communication of medical information. This discrete task is budgeted at more than $100 million, and is expected to take at least three years.

The Access Card project cannot – and should not – hope to duplicate or replicate or replace NEHTA's work by April 2008, when Access Card registrations are due to commence.

We recommend that the results of the Taskforce's research and consultations be provided to NEHTA, and NEHTA should be allowed to get on with its job, unrelated to the Access Card.

This feature lends itself to function creep

The very notion of incorporating medical information on the Access Card is itself an example of function creep – the use for a new purpose of a system established for a different purpose.

The Taskforce's Discussion Paper exposed disturbing ways in which stakeholders are already lining up to further expand the scope of the Access Card, such as by way of including personal information about blood group (p.8), HIV status (p.6), donor registration (p.7), childhood immunisation records (p.10), data from other medical registers (p.10), living will contacts (p.10), and even allowing access for law enforcement agency uses (p.12)!

We note that a submission to the Government on the first Access Card Bill, from the Australian College of GPs, also suggested that this 'emergency' health information should also include information about ethnicity (Aboriginality), and that the information should be able to be downloaded into GPs' records – without any mention of consent.

It is not too difficult to foresee a time in the future when, following an incident of terrible public violence or a controversial police shooting of a person with a mental illness, that pressure will be brought to bear on Government to make information such as mental or psychiatric illness a compulsory component of the card.

The only way to prevent function creep is to not have any discretionary space on the chip of the card, for use by the card-holder, the Government, or any third party.

Privacy implications overlooked

The Taskforce's Discussion Paper raises the spectre of third parties accessing 'emergency' health information from the card's chip, potentially in situations unrelated to medical emergencies.

However no mention is made of whether the same data will appear on the Government's Access Card Register, the "Secure Common Registration System", or SCRS. The privacy implications of this aspect of the proposal have been completely overlooked.

According to information published about the Register by the Government itself, the SCRS is proposed to have *all* the same information as is on the ID card's chip (*Access card at a glance*, "What information will the access card hold?, DHS website). That presumably includes the 'optional' emergency medical information.

In our submission to Discussion Paper No. 1 (see Appendix B), we asked the Taskforce the specific question:

> ***Will the 'optional' emergency contacts and health information also be saved on the SCRS?***

Our question remains unanswered.

The Taskforce's Discussion Paper also effectively suggests that medical information only be written to the chip by authorised medical personnel, in order to achieve the data verification and accuracy levels desired. While no doubt sensible, this makes a mockery of the Government's rhetoric that this is 'your card'.

The Discussion Paper makes no mention of important privacy considerations arising from having effectively a third area of the chip, controlled neither by Government nor by the card-holder. Issues which must be addressed include access and correction rights, obligations on medical personnel to check accuracy before entering data, and whose responsibility it is to ensure this data remains up-to-date. We also understand that concerns have been raised that criminal penalties applying to misuse of the card may not apply except in relation to the Commonwealth's area of the chip. If so this is an important privacy risk that ahs been overlooked by the Taskforce.

Each of these issues requires much more detailed consideration, in a timeframe simply not allowed for by the Government's stated intention to have all legislation ready by June 2007.