ACCESS CARD CONSUMER
AND PRIVACY TASKFORCE

Discussion Paper Number 2:

VOLUNTARY MEDICAL AND EMERGENCY INFORMATION

21 February 2007

TABLE OF CONTENTS

INTRODUCTION

In his address to the Australian Medical Association (AMA) National Conference on 27 May 2006, the then Minister for Human Services, Hon Joe Hockey MP stated:

> *"Importantly for the medical profession, there will also be space available for cardholders to voluntarily include vital personal information that could be used in medical emergency such as, next of kin, doctor details, allergies, drug alerts, chronic illnesses, organ donor status and childhood immunisation information. This information may save lives."*

In line with the Minister's commitments, the Access Card Consumer and Privacy Taskforce has explored issues related to the storage of this personal medical information with the aim of developing a protocol which could be introduced at the same time as the registration process for the access card commences, that is in April 2008.

Our deliberations have proceeded by way of the issue of a Background Information Paper in December 2006 which informed the discussions of a major round table panel which met on 15 December 2006, bringing together representatives of all areas related to this proposition. In addition, specific consultations were held between the Taskforce and peak organisations, including the Australian Medical Association.

This paper represents a distillation of those consultations and discussions and proposes a scheme for the recording of emergency health information and data on the proposed access card. It contains draft recommendations.

It is intended that this paper will be published on the Consumer and Privacy Taskforce publications section of the Office of Access Card website (www.accesscard.gov.au) and distributed to people and organisations who have already expressed an interest in the opportunities which such a scheme may offer. Once this paper has been circulated it is proposed to invite written comments, from both these participants and from the community generally, to be returned to the Taskforce by close of business on Friday 16 March 2007. These comments will then be considered by the Taskforce and a final report, with recommendations will be forwarded to the Minister for his consideration by the end of March 2007.

In several sections of this paper the Taskforce has indicated its particular interest in receiving public comments; however such comments are indeed welcome in relation to any part of this discussion paper.

The Taskforce will, in line with its normal practice, be recommending that the report to the Minister be made public. The determination of the exact scheme for recording emergency and medical data is a matter for Ministerial determination.

THE THRESHOLD QUESTION

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.

The customer controlled area of the card means that part of the chip, embedded in the physical card itself, which will be available for individual cardholders to use at their own discretion. Section 33 (a) of the *Human Services (Enhanced Service Delivery) Bill* 2007 establishes this area of the chip while section 40 provides a general right to use the access card for "any lawful purpose you choose." The exact amount of space (chip capacity) which will be available has yet to be determined but will be approximately one-third of the entire chip. Thus, the space available will depend on whether the chip specified in the card is of 64 kb capacity or some larger amount. In a 64 kb chip the customer controlled area will be in the order of 20 kb.

The threshold question which needs to be addressed is this:

- 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, and what information is merely convenient for a cardholder to have available to them by way of storage in the customer controlled area of their access card?

The answer to these questions will be what determines the most effective, efficient, customer-friendly and privacy protecting architecture to be put in place for the entry and management of emergency and health data on the access card.

The decision about what specific health and emergency data might be listed in the card is a considerably more complex matter than might have been anticipated. It is not simply a matter of storing anything or everything in an unselected fashion. This is because the data entered into the chip is data which is intended to be acted upon by other people. This is not data, such as the storage of a list or a telephone number or a birthday or a bank account number, where the action which flows from the storage of the data is action initiated by the cardholder themselves. This is data upon which other people act in good faith and where their actions may have significant (and potentially life-threatening) consequences for both parties concerned.

Because of this, there must, in the opinion of the Taskforce be a requirement, for the protection of the person who acts in good faith on the data provided by the cardholder, that a robust system of authentication and verification must be incorporated into the storage process. Without such a checking mechanism the storage of the data becomes less than useful, since third parties will either decline to act, or be restrained from acting, on the data, thus negating the whole purpose of its listing in the first instance. In the absence of such checking it would be possible to have a scheme entirely controlled and operated by the cardholder themselves, provided they expected no one else to do anything with or

about the data. In this respect health and medical data would be no different from any other.

If, however, the cardholder expects some third party to undertake actions to their benefit on the basis of the stored data then different rules and requirements must apply and be accepted.

Public comments on this issue are invited.

THE TASKFORCE'S RECOMMENDED SCHEME

The conclusion which the Taskforce has reached may be stated briefly:

The customer controlled area of the access card should contain a two-tiered system of emergency and health information:

- in the first tier, which should be accessible to anyone with an approved reader, there should be listed **only** that data which is absolutely necessary to facilitate the provision of emergency health treatment in a crisis situation;
- in the second tier, which should be PIN protected (and thus accessible only with the express consent of the cardholder) other medical and health data could be listed in accordance with the Recommendations which appear below;
- the Access Card itself could contain, on the surface, some symbol (such as the caduceus) to indicate that emergency medical data is stored in the chip so that no time is wasted in an emergency situation looking for information which may not be there in the first instance.

The definition of what may constitute information which is "absolutely necessary" in these circumstances is one which the Taskforce does not feel competent to state without the benefit of further expert consultation.

However, it seems to the Taskforce that individuals could consider including optional information on conditions such as epilepsy, asthma, diabetes and haemophilia. Similarly drug reactions and allergies which may be life threatening (eg allergy to penicillin) or medications being taken (such as anti-coagulants) and which might be relevant in an emergency situation could be listed.

Similarly, contact numbers, such as those related to details of any treating medical practitioners or enrolment in a Medic Alert-type system could be included at this level so as to facilitate speedy telephone contact which may be of assistance, although pressures of time and the immediate situation may preclude such checking.

It must be recognised and accepted that, under the Taskforce's proposed model, the information contained in Tier 1 is effectively information in the public domain.

Whether the information is stored in plain text or in some encrypted form is a matter requiring further consideration. This is a question which involves both the preferences of the cardholder and the specific operations of the relevant technology to be taken into account.

Public comments on this issue are invited.

To be of any use, the data must be readily and easily accessible. This means that anyone with an approved reader (including people in non health and emergency situations) will necessarily be able to view it.

A possible alternative – readers which have the capacity to over-ride PIN protected data is, in the opinion of the Taskforce, simply not practical. In the first instance it requires a method to establish who has access to PIN-override readers and secondly there is potential for the misuse of such devices.

As such, cardholders who chose to make use of this system must accept that they are putting sensitive personal information, effectively, into the public domain, and that this is something which they may be doing for the very first time.

Given this, the highest priority and consideration needs to be given to:

- what information is absolutely necessary in the case of an emergency;
- reducing the information in question to an absolute minimum;
- ensuring that there are effective sanctions available and applied in relation to people or organisations who breach privacy requirements inherent in the management of this sensitive data.

There are a number of other conditions which have been suggested regularly for inclusion in the first tier of the record, namely blood type and HIV/Hepatitis C status. The Taskforce would reject both of these examples.

Knowledge of blood type is generally not of assistance in emergency situations where plasma/fluids rather than whole blood is given and in hospital settings blood typing is a simple and speedy process.

There is no need for emergency/health personnel to know of a person's HIV/HCV status since it is expected that they will be applying universal precautions to deal with blood spills and possible contamination and because knowledge of HIV/HCV status leads frequently to the individual concerned being treated in an improperly discriminatory fashion and of the risk of having their privacy compromised.

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.

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.

Public comments on this issue are invited.

BACKGROUND PRINCIPLES AND PRACTICES

The more specific recommendations within in this paper have been developed against the recognition of certain background principles and practices already in place. These include:

- individual participation in any such scheme will always be voluntary and must be within the control of the cardholder
- emergency and health data stored in the access card must be absolutely accurate, reliable, up to date and capable of independent verification
- there are limits on the amount of data which can be stored in any system depending upon the capacity of the storage chip integrated into the card
- there must be a careful assessment and balancing of the maximisation of consumer choice and benefit against the need to protect individual privacy
- there are already well established schemes which record emergency health data, such as the Medic Alert bracelet/pendant system run by the Australian Medic Alert Foundation of which we need to be mindful
- a national organ donor scheme is in operation and is administered by Medicare Australia, a participating agency in the access card program
- many Australians already have created "living wills" or "advance directives" which are intended to give directions about the medical treatment which they are to receive (or which is to be withheld) in the event of the individual not being in a position to make such immediate decisions for themselves
- an effective scheme must also balance both privacy of sensitive personal medical data with the need for some of such data to be immediately and publicly available for use in emergency situations
- there must be consideration of the medico-legal issues which arise when people act in good faith on the information obtained from the access card. [These should, as far as possible, reflect current law and practice derived from similar situations where people act in good faith on information given to them orally in like circumstances.]

The Taskforce seeks to address some of these questions in more detail, and to derive formal Recommendations related to them.

Data Quality and Verification

The first issue is that of data quality and verification. Emergency health data might include information about allergies, medication, blood groups and the like. If this information is available to emergency and health workers, it is to be assumed that they might, in good faith, act upon it. This clearly has potentially life-saving or life-threatening consequences for the individuals concerned. Consequently there is a powerful and compelling argument that such data should not be listed on the chip without proper **verification or authorisation** by a medical practitioner. It should not be possible for any individual to list such data on their own initiative without verification – people might be unintentionally or intentionally inaccurate in the information they provide. Information may become outdated and again, potentially dangerous.

The Taskforce believes that it would be possible and practical to devise a system by which appropriate verification (for example by medical practitioners on a standard form showing provider numbers and other relevant data or by a pharmacist when changes in medication are being recorded) is provided before such information is entered into the chip. Similarly, data could be updated, to keep it relevant and contemporary with each visit to a practitioner.

It remains an open question as to whether there should be some charge for this service, and if so, who should bear that charge. The general position of the Taskforce is that, since this facility is being accessed at the choice of the individual cardholder it could be the responsibility of the individual to bear the costs associated with it.

Recommendation 3 : That no voluntary 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.

Public comments on this issue are invited.

This has a clear implication that the entry of such information cannot be done by the individuals themselves since this would allow the bypassing of the verification process. It means, that at least for Tier 1 information, data entry can be done only at an approved location and only from an approved and authenticated form. Ideally, such a form should also be checked to ensure that the information is not being fraudulently entered and that no improper alterations have been made once the medical practitioner issued the form. The Taskforce notes that this is standard practice in relation to the operation of existing Medic Alert-type schemes.

If this is the case, significant resource implications arise since it is unreasonable to expect participating agency personnel to be devoted to this exercise on behalf of individual cardholders. It may be such that data entry should only take place upon registration or when another transaction is underway and that consideration must be given to charging for this service, or on a visit to a practitioner, in exactly the same way as the Medic Alert-type services impose charges on their clients.

The Taskforce notes that in our consultations on this issue very complex medico-legal questions were raised but that it was made clear that it would be unrealistic to expect medical personnel to rely upon any such data which had been entered on the card in an unverified system. We were also advised that in the very recent introduction of a similar health-related card in Lombardy (Italy) such a verification system was mandated.

This is not just a simple matter of acting on the information available. Issues arise where a third party acts in an emergency situation and fails to either search for or act upon the information contained in the access card. In some circumstances (e.g. road trauma situations) it may not be either possible or timely to determine whether a person even has their access card with them (given that the law provides that it is not necessary to carry the card at all times), let alone take time to locate it and enter it into a reader.

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.

Public comments on this issue are invited.

Extent of Data Storage and Electronic Health Records

The next issue that arises is the extent of such information that might be listed. For privacy reasons, the Taskforce does not favour allowing an open-ended approach to this issue so that what develops is a quasi-electronic health record (EHR) established, effectively at random without appropriate standardisation or control.

The Taskforce draws attention to the fact that a significant number of submissions have canvassed a greatly expanded role for the access card in terms of linking it with other health records. The Taskforce is aware of the work being undertaken across various agencies to progress a national system of linked electronic health records assisted by the work of the National E-Health Transition Authority (NEHTA). The Australian Government has concluded that the access card program is not related to work being undertaken by NEHTA as this would represent a significant departure from the stated purposes of the access card.

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.

Data Linkage: Other Commonwealth Records

At present some 5.5 million Australians are listed in the Organ Donor Register which is administered by Medicare Australia. The Taskforce sees some merit in the individual cardholder being able, at the point of registration to give express consent to some flagging in the customer controlled area of the chip of a link to the details about organ donation which are already held in the Medicare controlled file.

Several submissions sought to establish a linkage between the access card and the register of childhood immunisations, although the case for this was not made out with any force or clarity. There are undoubtedly other registers of various health conditions or status which might fall in the same category but the Taskforce is in no position to determine which, if any, should be linked to the access card or whether this is simply a matter to be left to the discretion of the individual cardholder.

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.

Data Linkage: Non-Commonwealth Records

There has been an increasing interest by many people to provide for "living will" or "advanced directive" arrangements whereby instructions are left, by the individual about the sort of medical treatment they wish to receive, or to refuse, if they are rendered in a position where they are no longer capable of deciding this for themselves at any particular point in time. These directives are usually in the hands of a guardian, agent, next of kin or legal representative. Linkage from the customer controlled part of the chip to the contact point of the person/authority holding these directives on the part of the cardholder concerned seems to the Taskforce to be a proper way in which customer control and choice is enhanced. There is no necessity for the precise terms of any such directive to be listed in the chip if the contact point to ascertain this information is clearly accessible.

At present Australia has a system called Medic Alert in which some 300,000 Australians are enrolled. Medic Alert provides bracelets, pendants or badges to its members who wear them on a constant basis in a way which alerts those providing medical and emergency treatment to call the Medic Alert number and be provided with comprehensive health data about the subject person. Listing on the Medic Alert register follows a strict protocol which addresses all of the questions raised above about health status verification and the listing of emergency contact details. The Taskforce sees merit in an easy facilitation of the linkage between the access card and the Medic Alert register,

although this linkage must be confined simply to a flag which indicates that such data is available through contact with another database – the databases themselves must not be linked directly.

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.

Prescription Dispensing and Pharmacy Operations

Throughout our discussions and consultations there was considerable interest expressed by representatives of both the pharmacy profession and health consumers for the access card to have a significant role in the facilitating of pharmacy services and payments.

The Taskforce regards this as a discrete area for further discussion between the relevant Commonwealth authorities, consumers and the pharmacy profession, but not as a matter which needs comment or decision within the context of this particular discussion paper.

Such decisions will be made independently of the considerations of what health data individuals should be permitted to enter into their own customer controlled zone of the access card, and the Taskforce does not intend to canvass them further in this context.

Under the Taskforce's proposals pharmacists will be able to access records of the medications currently (or previously) being taken by the cardholder, provided that this data has been entered in the first place and provided that the cardholder consents to give access to this information. In consultation with the cardholder it may be possible for the pharmacist to assist in the updating of such records and doing this from terminals available and authorised within their pharmacies themselves.

Third Party Contacts

The listing of contacts of third parties, be they medical practitioners or friends/carers/family members to be contacted in the case of an emergency has privacy implications. There is clearly a benefit in being able to contact people in emergency situations and equally it is important to be able to identify if a person is either a carer for, or subject to the care of another person.

On the other hand, people so designated may not have been made aware that they are the contact point, or, that as a result of activity on the part of another party, some personal data about themselves has been entered into the system (e.g. their next of kin or relationship status or their private contact numbers). They may not have consented to be the contact point or to have this data listed in what, as we have noted above, is effectively a public and relatively easily accessible record.

A relative or partner might have been designated who would become inappropriate in a change of circumstances (divorce, separation, family dispute) which might not have been corrected/amended by the cardholder at the time that the emergency contact was triggered. Medical practitioners might be inappropriately listed, for example in circumstances where the individual concerned had services provided by more than one such practitioner, without the knowledge of others, and with a consequence that differing treatments/prescription had been authorised. We are aware that this matter has been addressed in other contexts (eg the listing of contacts in the Australian passport) but it is still one needing to be approached in line with best privacy protection principles.

Public comments on this issue are invited.

Children's Records

In the upcoming discussion paper on registration we will discuss various aspects of the rights of children to have their own access card and be able to operate upon it. We will also draw attention to the work being done in relation to children's privacy by the Australian Law Reform Commission as part of its general enquiry into Australia's privacy laws.

There has been public debate about the rights of children to their own access cards, although it needs to be noted that the Australian Government is not proposing to deny cards to children, nor to diminish their existing rights in this regard. The public discussion has centred primarily around the rights of children (those between 14 and 18 years of age) to have an access card in order to access medical services. As such, questions about the inclusion of voluntary health information on their cards needs to be considered in light of accessibility by parents, service providers (such as local pharmacists) or even law enforcement authorities if required.

In the observation of the Taskforce, many children and young people have quite different perceptions about privacy or about the sharing of personal information, than is the case with many (if not most) older Australians. [This opinion is confirmed by several surveys of consumer attitudes towards privacy protection.] The culture in which they have grown up, especially the on-line environment, encourages greater information sharing. Younger people also have more limited experience about the consequences of data sharing, as is only to be expected.

The Taskforce raises this specific issue since particular attention may need to be given to ensure that properly informed consent is obtained.

Public comment on this issue is invited.

Accessing the Emergency and Medical Data

Once information is listed, the question becomes exactly how such emergency data should be accessed. It has been suggested that such data should be PIN protected, but this clearly faces problems in emergency situations where the cardholder is unable to state/recall the PIN in question. It may well be that hospitals or ambulances would be equipped with readers which over-ride PIN protection, but this may be a less than optimal situation for the reasons which we have explained above. On the other hand, there are serious privacy issues arising from such data being open to public/plain view by every other (non-medical) person with access to the card for health and social service purposes, or as a result of their being in possession of a personal reader.

MANAGEMENT OF THE SCHEME

It will be obvious from the above that the entry of voluntary emergency and medical information into the access card scheme is not as easy an exercise as might have been contemplated. The medico-legal issues are such that there must be authentication and verification of data at least in the Tier 1 section of the database in the chip. This implies limits on the capacity of each cardholder to enter or alter the data in question. It suggests that data entry (and alteration) must be done by approved parties and that there may need to be some checking of original documents issued and authenticated by medical practitioners.

Whether this is done by the medical practitioners themselves using facilities available in their own surgeries (or in some instances pharmacies), by authorised officers in participating agencies or by some external third-party contracted for this specific purpose is an open question. The Taskforce understands that the Australian Government itself has no interest in running such a project and agrees entirely with this position.

The Taskforce believes that 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.

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

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.

Public comments on the issues of the management of the scheme are invited.

CONCLUSION

There is no doubt that the access card provides a series of opportunities for consumers, who are, under the legislation, the personal owners of the card in any event, to decide on the use of the card for a range of purposes and services of their own choosing.

The limits on these choices derive from a combination of the physical limits of the space available on the card for customer use and any restrictions imposed by the Australian Government for policy reasons (eg no direct linkage to electronic health records) or by law.

Against this enhanced range of consumer choice, cardholders need to be conscious of and balance the potential loss of privacy which is inherent in storage of personal data (some of it highly sensitive) which can, potentially, be read by third parties.

It is worth restating that the more data placed on the access card, whether that be mandated or voluntary data, the greater the risks to individuals when/if cards are lost or stolen, and the greater the attractiveness of the card to parties who might seek to steal/use it for improper, fraudulent or criminal purposes.

The storage of personal emergency and medical data differs from the storage of other data by virtue of the fact that, in storing the data, the cardholder (at least implicitly) does so on the basis that the data is there to be used by third parties, primarily for the assistance of the cardholder themselves. Thus, third parties have an interest in ensuring that if they act on the basis of data in the card, they are in a position to rely upon the integrity of that data and to be protected where they act on that data in good faith. In other words, the entry of personal emergency and medical data is not a matter exclusively for the cardholder concerned, and as a result, there is a public interest (discharged through the government) to ensure that any such system operates in accordance with the competing requirements of all parties.

The Taskforce hopes that this discussion paper has raised relevant questions worthy of further public debate, and it looks forward to receipt of those for its consideration before it provides concluded advice to the Minister for Human Services.

Public submissions can be made as follows:

Mail: Access Card Consumer and Privacy Taskforce
PO Box 3959
MANUKA ACT 2603

Email: a.fels@humanservices.gov.au

Closing date for submissions is cob Friday 16 March 2007.

All submissions should be in writing, and unless a request is made to the contrary, all submissions will be posted on the Consumer and Privacy Taskforce publications section of the Office of Access Card website.

Professor Allan Fels AO
Professor Chris Puplick AM
Mr John TD Wood

21 February 2007