



AMA

**AMA SUBMISSION
ACCESS CARD CONSUMER AND PRIVACY TASKFORCE
DISCUSSION PAPER NO. 2 –
VOLUNTARY MEDICAL AND EMERGENCY INFORMATION**

March 2007

**AMA SUBMISSION
ACCESS CARD CONSUMER AND PRIVACY TASKFORCE
DISCUSSION PAPER NO. 2 –
VOLUNTARY MEDICAL AND EMERGENCY INFORMATION**

The AMA welcomes the opportunity to respond to the Access Card Consumer and Privacy Taskforce's second discussion paper on Voluntary Medical and Emergency Information.

Recommendation 1 and 2

In its evidence to the Senate inquiry into the *Human Services (Enhanced Service Delivery) Bill 2007* the AMA supported the proposal for the Access Card to provide medical practitioners access to patients' emergency medical information and the necessity for that information to be reliable and trusted.

The AMA's view is that the two-tier proposal is likely to result in more people incorporating medical alerts within their card that will be of significant assistance to emergency physicians, doctors or indeed paramedics trying to save a person's life in an emergency situation.

The AMA supports **Recommendation 1** that the two-tier model be considered as a standard should individuals be able to provide voluntary emergency and health information that is then accessible through the Access Card chip.

The AMA supports **Recommendation 2** in principle. The AMA agrees that there is a need for consultation on this matter but is of the view that a solution that mirrors the current MedicAlert system may eliminate the necessity to be too restrictive in terms of information provided by the consumer and will at the same time resolve other issues around additional information that might be included on the card.

The AMA supports a model that mirrors the process as currently applies to obtaining a MedicAlert bracelet or pendant. Under this process, often on the advice of the patient's GP, the patient will obtain a MedicAlert application and is required to have the information included on the application form verified/signed by their GP. The verifying GP also advises the critical information that should be placed onto the bracelet or pendant. The application form is then sent to MedicAlert, which provides the bracelet or pendant to the patient. In applying to MedicAlert the patient is asked to also provide additional health information, next of kin contact and the verifying doctor is recorded. This information is held on the MedicAlert database and can be accessed when a health professional calls the 24 hour MedicAlert number and quotes the patient number contained on the bracelet/pendant. For emergency situations this provides doctors treating patients in emergency situations with vital trusted and verified emergency health information. It also provides information on next of kin, treating doctor and organ donor status.

For the Access Card the AMA would wish to see a similar process applied to information proposed to be included in Tier 1.

Data Quality and Verification – Recommendation 3

Recommendation 3 states that no voluntary medical information should be entered into any part of the Access Card without verification of the accuracy of that information by an approved medical *or other practitioner*.

It is the AMA's view that only a medical practitioner should verify the emergency medical information in Tier 1. It is unclear as to what the Taskforce means by "other practitioner". It is hard to imagine any medical information that is immediately necessary in an emergency situation being able to be verified by any other practitioner given this would relate to a diagnosed medical condition, prescribed drugs or diagnosed allergies. The veracity of the emergency information will be diluted should practitioners other than medical practitioners be given the role of verification for information in Tier 1. Under the current MedicAlert system only the treating doctor, with the patient's consent, can verify or change information contained in the MedicAlert

As to who should undertake the role of data entry it is the AMA's view that this be undertaken by one organisation in an approved location. This means that the same process for current MedicAlerts should apply. The application form signed by the GP (in ink or secure/authenticated electronic communication) should result in an approved organisation entering the necessary information. The type of information that should be contained in Tier 1 medical alert or otherwise is discussed further in this paper.

In terms of what organisation should have the role for data entry, it would in our view make sense to leverage existing infrastructure. In this context it is particularly important to note that the existence of an Access Card does not make MedicAlert bracelets or pendants redundant. The Access Card must not replace the current MedicAlert bracelet and pendant system but should complement it.

The AMA does not support a data entry role for the doctor. This would represent an inappropriate administrative role for the doctor that would impact on workloads within a practice. It would require new and additional work processes, training and possibly technical infrastructure.

Recommendation 4

The AMA strongly supports the recommendation that the medico legal issues arising from persons acting in good faith on the medical data contained in an access card must be addressed and clarified. The AMA would expect to be party to consultations around these matters.

Extent of Data Storage and Electronic Health Records - Recommendation 5

The AMA agrees that the Card should not be used to store electronic health records.

In terms of the linking to existing electronic health records, the AMA supports this recommendation only to the extent that it does not impede consideration of potentially significant future benefits related to use of the Access Card. Subject to public consultation

and debate this may include use of the Access Card as a key to shared electronic health records.

The unique patient identifier being developed by the National Electronic Health Transition Authority is essential to progress the reality of shared electronic health records. The inclusion of this completely separate identifier within the Access Card could be considered into the future. With a separate identifier, current technology and adequate legislative protection a virtually impermeable barrier can be established between the means to access an individual's shared electronic health record and the separate identifiers that link to Commonwealth databases for the current stated purposes of the Access Card.

The AMA would not support any recommendation that placed a barrier between consideration of significant and positive future uses for the Access Card, subject to the existence of a governance model at arms length from Government. As noted in other submissions the AMA considers the independence of such a governance body essential to transparent processes and community confidence around consideration of future uses of the Access Card.

Data Linkage: Other Commonwealth Records – Recommendation 6

AMA supports recommendation 6. In the context of information contained on the card and connection with other Commonwealth and, in particular, non Commonwealth data bases, it is important to note that the current MedicAlert system collects information on organ donor status and retains that information within its database. This must be taken into account should a model that mirrors the current MedicAlert system be considered.

Data Linkage: Non-Commonwealth Records - Recommendation 7

President of the AMA, Dr Mukesh Haikerwal, in his statement to the Senate inquiry, noted that emergency physicians, when trying to save the life of an unconscious patient consistently express concern at the lack of information available, particularly when they are faced with treating an unconscious patient. As one emergency physician pointed out, he is often left to dig through wallets and handbags trying to find any scrap of paper that might help save the patient's life.

There have been objections to the proposal that the card hold any health information. However, the AMA is perplexed as to why a person willing to wear a MedicAlert bracelet or pendant that is generally in plain view and certainly to a doctor, would be unwilling to do so on their Access Card. It appears to the AMA that these objections may relate to a substantial lack of understanding as to how the current MedicAlert system operates and the options that exist to mirror these processes with the Access Card.

The AMA is of the view that there are three options available that represent a mirroring of the current MedicAlert system. However, it is our view that these options should include the following rules:

- all information in Tier 1 is encrypted;
- information in Tier 1 can only be accessed through an approved reader;

- approved readers for Tier 1 are widespread in appropriate locations and with the appropriate providers.

In relation to Tier 1, public debate appears to reflect a perception that details of the individual's medical information must appear on the card. The AMA's proposed options demonstrate that this may not necessarily be the case.

Recommendation 7 appears to indicate that Taskforce considers that direct access to a medical alert database, similar to say the current MedicAlert databases may be an option.

The AMA's three options for information on Tier 1 that mirror the MedicAlert system are:

Option One – Medical alert only as information on the card.

Information on Tier 1 of the card would be notification that a medical alert exists. This is currently how the MedicAlert system operates. The MedicAlert bracelet/pendant acts to alert the doctor that an important medical alert exists. The doctor then contacts the medical alert organisation to obtain the verified information held by it with the consent of the patient. The same process could be applied to the Access Card. This would mean that all that is held in Tier 1 is a medical alert symbol and the patient's medical alert number. The doctor can then proceed to contact the medical alert organisation to obtain the necessary information contained on its database. This is information has been voluntarily provided by the patient in the knowledge that it may be accessed by a medical provider in the case of an emergency.

Even though a medical alert symbol does not in itself represent personal health information, in the interests of consumer confidence in privacy measures, it makes sense to the AMA to keep the fact of a medical alert separate (in Tier 1), encrypted and accessible only by an approved reader.

The Taskforce's view that information in the first tier would effectively be in the public domain is correct. Under this option, however, that information would simply be the medical alert symbol and the patient reference number. Tier 1 of the card would thus not contain any personal health information and as such reduce concerns around access to personal health information. Further this would be consistent with the Taskforce's Recommendation 5 that the card not be used to store electronic health records.

Consideration could be given to the card containing limited information such as the type of alert i.e. medical condition, medication or drug allergy alert but this could be optional for the consumer.

Combined with encryption and access restricted to approved readers, on the condition that this does not compromise ease of access in appropriate situations, this option represents a significant level of protection for the very minimal information contained on Tier 1 of the card. It is also less technically challenging than the second option below.

Option Two – Medical alert and critical information on the Card

This option represents a real mirroring of the current MedicAlert system in that the Card would include in Tier 1 the MedicAlert symbol, the patient reference number and the critical information as determined by the verifying doctor.

This is identical to the current MedicAlert model and is akin to the individual carrying a MedicAlert bracelet or pendant within their Access Card. However, the rules noted above provide a level of protection of this information in Tier 1.

While it is our view that adequate access protection can be imposed on the limited information in Tier 1, consumers privacy concerns may make Option 1 more attractive. Option 2 duplicates the current MedicAlert system in that it makes critical information available immediately, while Option 1 requires contact with the medical alert organisation for access to the relevant information. While this occurs in the current MedicAlert model the treating practitioner does at least have at hand immediately critical information.

Again the AMA would ask opponents of this type of option why a person willing to wear a MedicAlert bracelet or pendant would be unwilling to carry an identical item on their Access Card, particularly with significantly greater levels of security of access to the information held on the Card and that on a completely separate database.

Option Three - Link to a medical alert organisation database.

This reflects the recommendation within the Taskforce's discussion paper but provides direct access to the database of the medical alert organisation using the Access card.

While this is an eminently sensible suggestion it may be that, given the privacy and technical challenges will be more complex, this option could represent a second phase of the model. Options 1 and 2 above, represent models that can be implemented with relative ease, possibly as phase 1, and in mirroring current processes that are acceptable to consumers reduce some of the contentious issues that may surround direct access to the data base using the Access Card.

All three options, resolve a number of other issues. They ensure that the database for emergency information held by the medical alert organisation is separate from any other databases being accessed through use of the card. It thus simplifies the capacity to develop rules around prevention of any data linkage from that database with Commonwealth databases, assuming a private sector organisation manages that database. Further, other relevant information critical in an emergency, such as next of kin, treating doctor, and even organ donor status can be held by the medical alert organisation database, along with other non critical health information including medications, as is currently the case with MedicAlert.

There is a necessity for consultation with the profession on what constitutes important health and emergency information, as suggested in the Taskforce's Recommendation 2. This would particularly be the case should Option 2 be considered, although presently the verifying

doctor makes that decision when verifying a MedicAlert application. However, by mirroring the current MedicAlert model it does mean that the information available in Tier 1 is not necessarily restricted by the size of the chip – this is particularly the case for Option 1. And again by mirroring the MedicAlert system and applying additional access security it strongly protects the information in Tier 1 and ensures the database that contains the details of the medical alert is completely separate from the Commonwealth databases.

If a patient did not have a reason to have a medical alert Tier 1 could, however, also hold useful information in the case of a health emergency, such as doctor and next of kin and perhaps even organ donor status. Allowing organ donor status to be held in either Tier 1 and/or the medical alert database removes the necessity for linking the card to the Medicare organ donor register.

Health Information in Tier 2

Other objections to the proposal around health information on the Access Card have been raised around information stored by the consumer on the second tier. In the AMA's view the second tier has to be considered in the same way as an individual's handbag or wallet. The consumer might store health information in that section if they wish and if that information is held there the emergency physician can only rely upon and trust that information in the same manner he or she would the scraps of paper or information contained in a patient's wallet. Under the two-tier proposal, however, the doctor may have access to some trusted information in Tier 1 in addition to the information in Tier 2 - the veracity of which is not reliable.

It is our view that given the type of information a consumer may include in Tier 2, including health information, it should be encrypted and protected by a PIN. Consideration could be given to allowing PIN bypass for approved readers where the service is directly related to medical providers but this may give rise to privacy concerns and create unnecessary complexities. It remains preferable that Tier 1, containing critical and verified information, is the first "port of call" in an emergency situation.

Prescription Dispensing and Pharmacy Operations

The proposal that pharmacists be able to access and change records of current medication records appears to be inconsistent with Recommendation 5. Medication records are health records. Tier 2 may provide this option to consumers but the information could not be considered reliable without verification by the treating GP. Pharmacists could only input information into the card about the medications they have dispensed. To suggest that a pharmacist is able to do more implies that pharmacists have access to shared electronic medication records or would update the card by linking with the PBS database – this is not and should not be the case.

There are also issues around the currency of that information, an issue that has consistently challenged the development of electronic medication records. The reality is that Tier 2 is a section of the card where the consumer chooses what they wish to put on their card and medications may be the type of information they wish to store. Again this would be similar to consumer maintaining a list of medications on a piece of paper in their wallet or handbag and while potentially useful information, it cannot be relied upon.

Third Party Contacts

The AMA would simply wish to make the point under this item that the current MedicAlert system obtains information on next of kin and maintains this within its database for access in times of emergency. Further the doctor that verifies/authorises the information in the MedicAlert is identified as the medical practitioner contact within the database. It is our understanding that this information is updated annually.

Where a person does not have a medical alert within the card there may be points of time or during specific card processes or contacts that the consumer is asked whether information contained in Tier 1 of the card needs to be updated.

Children's Records

The AMA is of the view that the same privacy protections extended to adults should be extended to young people who have their own Access Card. It is important to note that only 2.5% of people under 18 years old currently have their own Medicare Card. As part of that figure only 1.5% of those people are under 15 years old.

It is our understanding that a young person who, for example, may be away from their parents attending school, can remain on their parents Access Card, and will, as is currently the case, be provided with a duplicate of this card. This is essential to allow the young person to access health care when they are not with their parents. Where a young person is still on the parent's card, under the current guidelines under the Health Insurance Act those parents may, access information held by Medicare Australia on their child up to the age of 16 with the child's consent.

Accessing the Emergency and Medical Data

The AMA finds this issue somewhat perplexing in light of the proposal that the consumer section of the chip be divided into two sections. The Taskforce's recommendation on a two-tiered approach states that the first tier should be accessible to anyone with an approved reader. The question goes to whether there are different levels of approved readers depending on the type of information that it is necessary to access in different parts of the chip. For example, if a consumer is dealing with a Commonwealth agency on a non-health issue, does that approved reader provide access to both the section of the card that enables payments and services to be rendered or is it envisaged that it will also provide access to Tier 1 information? If this is the case the less information in Tier 1 the better and hence the attractiveness of duplicating the medical alert model outlined in our Option 1.

However, if different levels of access for approved readers were available this may offer a solution. For example, Centrelink may have an approved reader that provides access to the section on the card that permits payments to a consumer but the reader does not provide access to Tier 1. A doctor or hospital reader may have access to the area that facilitates Medicare payments but their readers also have access to Tier 1.

PIN protection for the consumer area of the chip implies a single PIN for access to Tiers 1 and 2. While a PIN bypass for emergency access is an option this implies that information not immediately necessary or even relevant in an emergency in Tier 2 of the consumer section will also be able to be viewed. The AMA is of the view that access to Tier 1 should be through an approved reader and should not be PIN protected, otherwise it completely eliminates its value in an emergency situation.

The AMA is of the view that Tier 1 should be accessible through an approved reader and Tier 2 should be PIN protected.

Management of the Scheme – Recommendation 8 and 9

The AMA agrees with 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. As we have noted in other submissions, however, the Office of the Privacy Commissioner must be adequately resourced to undertake these tasks.

In regard to Recommendation 9 the AMA is concerned to ensure that the scheme to which the recommendation refers relates wholly to the model by which emergency medical and health data is obtained, retained and accessed. As to whether this is administered in the public or private sector must be a matter for strong consultation by the Government. Ultimately the AMA view on this matter will depend on the model selected for ‘the scheme’.

For further information on this submission please contact Ms Julia Nesbitt, Director, General Practice and E-Health Department on 02-6270-5462