

AMA SUBMISSION

**RESPONSE TO
DISCUSSION PAPER NO. 1
ACCESS CARD CONSUMER
AND PRIVACY TASKFORCE
HEALTH AND SOCIAL
SERVICES ACCESS CARD.**

July 2006

**AMA SUBMISSION ON DISCUSSION PAPER NO. 1
ACCESS CARD CONSUMER AND PRIVACY TASKFORCE
HEALTH AND SOCIAL SERVICES ACCESS CARD.**

Issue 1 The Right of Choice

The question of the consumer's right to authenticate their identity by other means goes to issues around the purposes of the card and the embedded consumer identifier. It is the AMA's view that in order to provide consumers with protection afforded by the current privacy regime, particularly the Privacy Act, clear purposes for both the card and the identifier must be established. In that context, the Privacy Act can protect against other uses, particularly in relation the use of the unique consumer identifier.

There is a need, however, to discern between the purposes and uses of the card and the purposes and uses of the consumer identifier. This cannot be the Medicare number as current privacy legislation prevents the Medicare number, as a Commonwealth identifier, from being used for purposes other than that for which it was established. Putting aside all the facts around limitations of the Medicare number to represent a unique identifier, the failure to include a separate identifier within the card would restrict any further functionality beyond those purposes related to the Medicare Number.

During the development and piloting of the Federal Government's MediConnect electronic prescription record the Department of Health and Ageing consistently advised that they would use the Medicare number as the patient identifier. The AMA just as consistently advised that this would represent a breach of the Privacy Act in relation to the use of Commonwealth identifiers. The AMA became particularly concerned when the Department advised it would legislate its use in MediConnect thus overriding the limitations of the Privacy Act. The AMA wrote to the Federal Privacy Commissioner who indicated his support for the AMA view. In particular there was real concern that the Government's solution was to simply seek to override the Privacy Act and the consequences such an approach would have on the credibility of the Privacy Act.

The purpose of relating this piece of history is to emphasise the need to focus not only on the Access Card itself but the identifier that will ultimately be embedded within the card. To not embed an identifier will limit future functionality. Further it would be inconsistent with major work being undertaken by the National Electronic Transition Authority in developing a unique consumer identifier and a consumer directory as well as parallel provider identifiers and directory. In the 2006/2007 Budget the Federal Government allocated \$70.2 million to a total COAG package, announced on 10 February 2006, of \$130 million to deliver:

- A unique healthcare identification number for all individuals (\$45M);
- A unique identification number for every healthcare professional (\$53M);
- A common language for health communications (\$32M).

In the AMA's view this discussion paper does not adequately discern between the card and the embedded identifier. Each may have different uses. The most significant risks to privacy relate to the use of the embedded identifier. The MediConnect experience, particularly the Tasmanian Smartcard initiative demonstrated to the AMA the very significant requirement to make this distinction. In the Tasmanian case Medicare Cards, containing a visible Medicare number, continued to be used for the purposes for which they and the Medicare number were

created. However, it was the embedded additional identifier that allowed expanded functionality for the Medicare Card (as opposed to the Medicare number).

On the issue of rules and limitations about the data, which cardholders might voluntarily choose to record in the chip, there is a real concern about the reliability of that information for the purposes of health care and particularly health emergencies.

The AMA has participated in numerous debates over the capacity for consumers to record information such as allergies, medications etc into specific fields in health records for example. The fact is the usefulness of the information is related to the reliability of the source. For example, from a doctor's perspective the consumer is not always a reliable source of information on allergies. Many consumers incorrectly translate adverse reactions as "allergies".

While the field may be voluntary and the consumer may record whatever they wish it would be risky for the medical profession to rely on that information, particularly where a patient is unconscious or unable to confirm details.

In our view the field is best used for the recording of emergency contact information. This may not only include family contact information but also possibly regular GP or treating specialist.

There is a case for finding a way to incorporate key medications where the absence of that information is life threatening. Warfarin is a good example. There remains the problem of verifying the accuracy of that information where the consumer is permitted to record it in the absence of any types of protocols.

There are clearly certain types of information that if reliable could be life threatening if ignored. It is likely that where there is doubt around the reliability of that information a doctor in an emergency situation will make decisions on the basis of that information until it can be verified. This in itself can create risks.

The capacity to store additional information is a secondary function of the Access Card. Focussing on any secondary functionality risks diverting debate from the current key proposed functions of the Access Card. A secondary purpose or function must not drive the technology or the processes currently under consideration. The reality is that some of the limitations of the Access Card, in terms of potential future functionality, are really about the current state of play in relation to developments around electronic health and medication records. Until these developments become a reality in terms of providing reliable and accurate patient health information, the capacity for consumers to record health information on the Card will remain a secondary function. The benefits do not link to the primary purpose.

The sooner access to health and medication records becomes a reality the sooner consideration of expansion of the Access Card functions might be considered. These functions would, however, be unlikely to be related to the information stored on the card, particularly by the consumer, but to its role as a "key" to allowing the right people, at the right time and in the right place to access relevant information in the interests of quality patient care.

Issue 2 The Right to and Protection of Privacy

The AMA acknowledges the statutes that provide privacy protection as noted in the discussion paper. An important point arises in relation to Section 135AA of the National Health Act that protects the separation of PBS and MBS databases. In November 2004 the Federal Privacy Commissioner invited submissions related to a review of Section 135AA and stated that a number of factors tend to suggest that a review was timely, including:

- developments in information technology which may have bearing on the handling of electronic records;
- the increasing use of information technology in the planning and provision of health services; and
- community attitudes and expectations regarding the handling of personal information, and in particular sensitive health information, may have altered during this time;

The AMA's submission to the Federal Privacy Commissioner noted that:

“It is the AMA's view that the development in information and communications technology has created a significantly greater potential for privacy intrusion through data linking. In that context it is of more importance today that the law and, in particular the MBS and PBS Privacy Guidelines, continue to stringently protect the separation of MBS and PBS data. In light of current technological developments and the potential risks to privacy from a greater capacity for data linkage, there may in fact be a case for strengthening the Guidelines.”

In the view of the AMA, the Information Privacy Principles in the current Commonwealth *Privacy Act* 1988 would not offer adequate protection for holders of the Access Card. We have already referred in our response to Issue 1 to the willingness of some government agencies to override the *Privacy Act* by legislation where it suits their purpose. Any new legislation drafted for the Access Card would need to contain an express and unambiguous statement that it was not overridden by other legislation - although this would not, of course, prevent later legislation from providing the opposite just as clearly.

In particular the AMA would be concerned about the operation of IPPs 2, 10 and 11.

IPP 2 currently provides that information may be used for collateral purposes if the person is made aware of these purposes at the time of providing the information. Most government forms now contain an "IPP2 clause" which stipulates the purposes for which the information may be used. The consumer is given little choice about that use of their information if they want to access whatever benefit is conferred by filling out the form. IPP 2 is currently used to circumvent protections in the Act on the basis that it is sufficient simply to inform the consumer that their information is going to be used. IPP 2 together with IPP 10(1)(e) is also used by government agencies to run audit and evaluation programs of which the consumer is never informed but which are considered by the agency merely collateral to the running of the program for which the information was originally collected.

IPPs 10 and 11 provide exemptions under the *Privacy Act* for the use and disclosure of personal information. One of those exemptions is for "consent". This is problematic because consent is rarely given with complete freedom. Usually consent is obtained on the basis that the person cannot proceed with the transaction or obtain the benefit unless they give their consent to the particular use or disclosure of personal information. If this exemption were to

be adopted in relation to the Access Card, the AMA would like to see the IPP amended to say that the exemption for consent applies only where the benefit or transaction is available to the consumer completely irrespective of whether they provide consent to the use or disclosure of their personal information.

IPPs 10 and 11 also contain an exemption to the prohibitions on use or disclosure of personal information "where required or authorised by law". In recent years, the Australian Government Solicitor's Office of General Counsel (by whom most government agencies are guided) has taken the view that an exception on a prohibition is sufficient to meet the condition "authorised by law". That is, where a secrecy provision in other legislation does not apply in a certain circumstance, then this is considered to "authorise" the disclosure of personal information for the purposes of IPPs 10 and 11. An example is the issuing of a public interest certificate under section 135A(3) of the *National Health Act*. This means that the protection of the IPPs is dissolved by the stroke of a pen by an agency that considers it expedient and has a legislative secrecy provision to which exemptions can be found.

It also means that the Privacy Commissioner has limited ability to control the use and disclosure of personal information as each government agency can simply create its own overrides through amendments to its own legislation. For example, recent amendments to the secrecy provisions in the *Social Security Act*, pushed through on the coat tails of the Welfare to Work reforms, significantly lessen the protection of personal information held by all the administering departments.

IPPs 10 and 11 also contain exemptions to the prohibitions on use or disclosure of personal information for the protection of the public revenue. This gives a very broad discretion in relation to the sort of information that would be found on the Access Card.

The AMA submits that:

- there should be legislative protection for the information held on or accessible through the Access Card,
- this protection should not be able to be overridden by provisions in other legislation,
- the protection should not be able to be waived by consent unless the consent is absolutely voluntary
- the uses to which information can be put should have absolutely clear limits.

It is also essential to ensure that data held on or unlocked by the card is exempt from Freedom of Information legislation except to the person to whom the information relates.

There must also be adequate security clearance for the officials who will have access to the information, and compliance with legislative secrecy and privacy provisions must be rigorously enforced. At the moment, most legislative secrecy provisions contain criminal penalties of up to two years in prison, but in reality these are almost never enforced. If the public is to have faith that the information will be protected, any breaches of privacy will need to be vigorously pursued, *pour encourager les autres*.

Issue 3 Customer Benefit and Customer Control

The AMA has been consistent in its view that the key to privacy of health information is providing the patient with a level of “control” on who accesses their information, when and where. The Access Card as currently proposed does not include any e-health functionality. In this regard it does not provide access, assuming current legislative provisions remain in place, to any information not currently available.

The issue of control over access to sensitive health information will be of monumental significance when discussion occurs into the future around potential e-health functionality, including in relation to access to electronic health and medication records.

As the Access Card is likely to operate as the key and is unlikely to store information, it will not be the card or the identifier that is the issue but the policy and processes agreed around the information to which the card provides access.

In the context of MediConnect for example the debate was not around the technology that created the record but around who had access, under what circumstances/rules, controversial issues related to the capacity of the patient to “mask” certain information in the record and consent for emergency override.

Issue 4 Making The Right Technology Choices

AMA recognises the value of Smartcard or chip technology in electronic systems, particularly in terms of authentication. There is little doubt that the rapid advances in technology mean that there are risks that electronic initiatives can become quickly outdated. Smartcard technology is being used successfully throughout Europe, Singapore, Hong Kong and in many American States. It is our understanding that the Access Card will be based on EMV¹ that is the global interoperability standard that facilitates the introduction of Smartcards into international payment systems. Further it is our understanding that the unique identifier may be a derivative of the current Medicare number but must be increased to 16 digits to ensure it is International Standards Organisation (ISO) compliant.

When the Government announced “Smartcard” trials related to HealthConnect in Tasmania in 2004 the AMA expressed its significant concern that no serious work had been undertaken to determine whether Smartcard technology was the best technology for the purposes of the Tasmanian Smartcard. The Tasmanian experience is a very good example of what not to do in relation to implementation of technological solutions. The first mistake was the absence of any authoritative research to support the choice of Smartcard technology, the second was the absence of any clear purpose for the Smartcard and the third was the absence of supporting technology that operationalised the functionality beyond the existing Medicare Card.

AMA has consistently warned Government that the community maintains a healthy suspicion around new technology and its purposes. In that context investment of taxpayer money into such initiatives must be thoroughly researched, including community consultation. There is no doubt that when the promises of electronic health initiatives are not delivered or mistakes are made scepticism translates into poor community uptake and low levels of acceptance.

¹ Europay Master Card Visa Integrated Chip Card Standard

This is particularly the case when one is dealing with sensitive personal information such as health information. The AMA has argued that the wrong choices in both technology and policy that lead to a privacy breach, for example, have the potential to put the Government's e-health agenda back by many years.

Function Creep

Function creep is always one of the major dangers around the development of e-health initiatives. It not only relates to expanding the purpose or function of the card but most importantly the use of that data accessible through the card or identifier. The greatest threat in function creep is data linkage beyond the original purpose.

The AMA is of the view that certain measures may protect against function and data linkage creep.

A legislated clear purpose/function for the embedded Access Card number (which we assume will be the unique consumer identifier) to ensure any expanded use is protected under the current privacy regime is essential. Dangers of function creep relate predominantly to the use of the consumer identifier contained in the card and the significant capacity to link vast amounts of data through that identifier where restrictions (technical, legislative or policy) do not exist or are inadequate.

The development of the Access Card and related systems must be focussed on the prime purpose. Too often e-health initiatives have failed because of the ongoing addition of secondary purposes during the development stage. The expansion of 'purposes' in the development stage impacts not only on the technological developments but on the parallel development of related processes and policies surrounding its use. In relation to MediConnect, for example, the secondary purposes around the Government's desire to access a broad range of data and data linkage options, overrode the stated primary purpose of improvement to health outcomes. This was so dramatic that ultimately it was difficult to discern the relationship between much of the related policies and process to the stated primary purpose, improving health outcomes.

In the AMA's long experience in participating in a range of e-health initiatives the major pitfalls and barriers are not related to the technology. They are directly related to the policies associated with its use, the use of the data it potentially delivers and the relationship of these to the primary purpose.

Governance

Governance is a significant issue in preventing the diversion or perversion of the technology into doing something quite different to that for which it was created. In this regard the AMA maintains a significant level of discomfort that the role of overall governance and management of the Access Card should be undertaken within Government.

In the AMA's view governance and management should be as independent as possible from Government. This is particularly important into the future. A level of confidence may be deliverable in relation to the current concept of the Access Card with its limited functionality. It is future e-health functionality, however, and the way in which that is progressed that will give rise to concern in the community.

It is the AMA's view that the Government itself represents a key risk in the potential diversion or perversion of the purpose of the Access Card. This is particularly the case because the Government will "own" the card and also hold the data that it will at times have a strong desire to link.

Consultation

Further the Government's track record on community consultation on e-health issues is poor. In 2004 all of the e-health stakeholder advisory groups and/or development groups were abolished and direct consultation on e-health matters ceased. NEHTA was established and in the context of new national governance arrangements for e-health that included the Australian Health Information Council all representative consultation ceased. The AMA's E-Health Summit in December 2005 in which the medical profession and major private companies participated, confirmed the AMA's view that in broad terms there was significant dissatisfaction at the level of consultation by Government. At the jurisdictional level consultation on e-health initiatives is at best patchy but largely unsatisfactory.

The Government, and indeed possibly the Taskforce, will need to convince the public that placing the responsibility for financial management and overall governance within Government is a privacy enhancing measure rather than a privacy risk.

Besides privacy, however, the AMA has some concerns about the capacity of Medicare Australia to manage this project in both technical and policy governance terms. The Government's track record is not good on e-health development and implementation. Medicare Australia has not demonstrated itself to be willing to embrace policy change around e-health and its consultative processes have deteriorated significantly. We also have concerns that Medicare Australia may not be adequately engaged or across the key e-health developments at the national level, such as the work of NEHTA. NEHTA's standard setting work will dramatically impact on the manner in which the card works from both a technical and policy perspective, and its potential functions into the future. A comprehensive assessment of Medicare Australia's capacity to manage this initiative is essential.

It is the AMA's view that a critical role for the Access Card Consumer and Privacy Taskforce is to establish a process that governs the manner by which any expansion of the Access Card's functions are managed. This role may include the consultation, development and implementation of strict limitations on particular types of functions into the future.

Importantly any proposed expansion of the Card's functions will require transparent consultation processes, not only with the community, but also with other Federal Government Departments. In terms of proposals for future expansion to incorporate e-health functionality these are most likely to come from the Department of Health and Ageing. In that context the community must be able to "trust" that Medicare Australia is not only capable and willing to implement strong and transparent consultation processes but also has the capacity to manage and to defend the principle of protection of individual privacy. The question thus arises as to "authority" around decisions related to expansion of functionality into the future.

We agree with the statement in the discussion paper that:

“The Australian public’s trust will be very much dependent upon the extent to which it is accepted that the operations of the new Access Card are monitored and supervised by a body which is independent of the participating agencies.”

There is little doubt that development of the Access Card is a balancing act – all about ensuring the architecture of the card is capable of supporting other agreed and desirable applications but at the same time delivering public confidence and trust that future functions will be determined and controlled in a transparent, open and consultative manner.

It is important to ensure that we do not end up being captured by the owners of the technology and that full intellectual property in the system vest in the Commonwealth.

Issue 5. Authorisation and Accountability

The AMA is of the view that legislation is the only way in which the operation of the Access Card and the protection of information can adequately be safeguarded. The legislation should be separate from existing privacy and social security legislation so that it cannot be diluted by amendments to other parts of this legislation. For the same reason, the Access Card legislation should state specifically that it cannot be overridden by changes to other legislation.

Of course this will not actually prevent it being overridden if later legislation expressly provides for that; there must be some way of reassuring the public that the privacy of their information is immutable. That may be difficult to achieve given that the Government has recently seen fit to override so many existing individual rights in the context of national security laws.

It should be clear in the legislation what avenues people have to obtain an Access Card, what obligations the government has to help people acquire one (particularly those who are disadvantaged by reasons of geography, disability, literacy and the like), and what options are available for those unhappy either with a decision to refuse a card or with the accuracy of the information stored upon it.

Subsidiary issues, such as the circumstances in which a minor may have a card, should also be considered. Associated with this is the issue of whose card a child is registered on when parents share custodial arrangements, particularly in view of the forthcoming Parkinson's reforms to the family law system and the greater responsibilities of each parent. Having the child registered on both cards creates obvious problems of duplication; having the child registered on only one may hinder the ability of the other parent to acquit their responsibilities when looking after the child.

It will be essential that from the very introduction of the card there should be vigilant and dedicated resources for monitoring abuse of cards and breaches of the system. There should be substantial criminal penalties for offences such as fraud and misuse of information, and, importantly, the system will lose credibility if these are not penalised appropriately. At the moment, existing sanctions for breaches of secrecy provisions are almost never invoked. This will need to change if people are to have faith in the integrity of the Access Card.

At the same time, if fraud or identity theft is detected, it must not be unduly difficult for a person to undo the damage that may have been done to their finances and reputation. Where

a person's identity has been stolen, there should be some way in which they are readily able to demonstrate that this has occurred, and have their card reissued and entitlements restored with minimum fuss and disruption.

This leads to the question of what happens if a person loses their card. Presumably it should not be possible for someone to merely ring up and report it lost and order another. Some method is required for people to be able securely to report the loss of their card and obtain another quickly. This will be particularly difficult where for reasons of geography, disability or other disadvantage it was difficult for the person to demonstrate their identity for the initial issue of the card. There will also need to be some provision for people who may be vulnerable, such as those in institutional care, to ensure that carers or relatives cannot easily manipulate their card. There is anecdotal evidence, for example, that in some communities social security entitlements are managed by publicans or shop owners and recipients draw down on their own entitlements. There should be severe penalties for any person who takes possession of another's Access Card for this purpose.

Administrative arrangements should be isolated from other government operations. This is particularly so in light of recent amendments to the social security legislation which purport to allow disclosure of any information (not just social security information) held by any department administering the legislation, for a variety of broadly-drawn purposes. It must be quite clear that the arrangements and protections attaching to the Access Card cannot be affected by other developments in the way in which departments hold and manage information.

Only appropriately authorised persons should be able to access the information on the card, depending on the level of detail they can access and the use to which it will be put. There should be a tracking system to monitor who has accessed what information. Ultimately, though this might be very difficult to design and administer. It would be preferable if people could access their own information and be able to view who else had accessed it and for what purpose. It is recognised that it would be difficult to create a system that was both highly secure but also accessible to all card-holders (although internet banking models might provide a guide).