AMA Submission to Independent Review of Health Providers' Access to Medicare Card Numbers

August 2017

The Government's response to the alleged sale of a small number of Medicare numbers on the dark web needs to be proportionate. In developing any policy changes, it must ensure that patients, particularly vulnerable patients, do not have their access to medical care reduced. It must also recognise the significant red tape burden already faced by medical practices and not add significantly to this.

While not seeking to downplay the significance of the alleged sale of Medicare numbers, the allegations must be put into perspective. The AMA understands that 75 Medicare card numbers were sold on the dark web and this needs to be put into context. Every day there are 45,000 provider interactions with HPOS, an estimated 27,000 HPOS confirmations of Medicare details and in the last year 148.8 million GP services claimed against Medicare. There is no evidence of a systemic problem and no evidence that patients' health information has been compromised.

It is important that systems are in place to protect Medicare data and all indications would suggest that current arrangements work relatively well. Medicare has in place its own safeguards and medical practices take the privacy of patient information very seriously. Any changes to current arrangements must be targeted at improving the security of data, while at the same timing erring in favor of giving patients access to care. Indigenous patients, homeless people, people with severe mental health conditions and those living on low incomes already face significant barriers to accessing care and we should not add to these.

Importantly, if there are obvious flaws in the Governments own systems, the solution to these does not lie in burdening medical practices with extra red tape.

The HPOS system works relatively well for practices, evidenced by the high volume of Medicare number confirmations processed through it in comparison to the Provider's Enquiry line (10 million online vs 558,000 by phone per annum).

Systems such as HPOS, must continue to support medical practices to provide care for patients otherwise it will undermine the Government's efforts to transform the way Medicare does business with practices in an increasingly digital age.

Response to discussion paper

HPOS

<u>Moving HPOS authentication from PKI to PRODA within three years</u>

The AMA supports the move to PRODA as soon as possible. To encourage this, the Government needs to ensure that PRODA meets the needs of practices by enhancing the functionality of PRODA to enable secure messaging, business transactions and data exchange between providers and Medicare Australia and other authorised parties approved by Medicare Australia.

Given the commitment to modernising Medicare systems, this represents a logical next step. It ensures provider systems flexibility, while retaining capability for secure interactions with Medicare Australia and the Department of Human Services.

In a mobile, digital, online and cloud based world physical certificates tied to a physical machine are restrictive and limiting and, as the alleged breach has identified, are vulnerable to misuse and breaches of security.

Reviewing the HPOS Terms and Conditions

Any changes to HPOS Terms and Conditions must not increase the administrative burden on providers.

HPOS provides health professionals and their delegates with streamlined and secure access to Medicare Australia and Department of Human Services programs, services, tools and resources. This not only facilitates provider engagement with the Department and its programs, it also supports secure transfer of data and timely access to information.

If HPOS becomes more cumbersome providers will cease to use it. This would add significantly to the costs of business for Government and providers alike through the use of less efficient process and systems.

In addition, it could be expected that patient access to services, particularly bulked billed services, would be impacted. If general practices are not able, for example, to readily access a patient's eligibility for Medicare, or to verify a Medicare rebate is payable for a particular health service (e.g. a Health Assessment or GP Management Plan) they are more likely to bill the patient directly to ensure they are not out of pocket for providing the service.

Suspending inactive PRODA accounts and PKI site certificates

The AMA is uncertain what problem this proposed action would be addressing. Inactive PRODA or PKI site certificates are of little threat to the system as no one is using them.

There are a number of reasons why PRODA or PKI certificates may be inactive but still be required, such as a holder may be on maternity leave, or extended sick leave, or temporarily not providing services or out of the country.

PKI certificates in particular are onerous to obtain and install. Once a provider has set up their details and delegates they may have no need for further interaction unless any of their personal or practice details change or a change to their delegations is required. Most interactions with HPOS are undertaken by provider's delegates. Particularly, in the case of general practitioners, whose time is far better spent caring for patients then completing administrative tasks on behalf of the Department of Human Services.

Suspending PRODA or PKIs of practice principals could cause their delegates to lose access, adding unnecessary administrative burden to practices and delaying the transfer of information between practices and the Department.

If suspensions are implemented the AMA would strongly encourage the Department to ensure that holders are appropriately notified and given the opportunity to confirm their PRODA account or PKI is still required. Any suspension should be easily reversed.

Adding an expiry period for delegations in HPOS

Rather than implementing blunt administrative rules that expire delegations, the Department could provide a better service to providers by regularly providing a list of their delegates so that they can review and confirm their currency.

Further conditions for batch Find a Patient requests

Batch requests are made generally for the purpose of claiming bulk billed items or processing claims on behalf of the patient. There is not enough information in the discussion paper to inform a discussion about the need for further conditions on batch requests. It would have been useful if the discussion paper could have provided some information as to how often batch requests are run, by whom and what the average volume of requests is. Information, such as this could then be used as the basis for any discussion about reducing the number of requests allowed.

The AMA would expect that any unusual behaviour from a practice with regards to batch requests could easily be identified by the Department of Human Services and investigated.

Provider enquiries line

Strengthened telephone security check

The AMA believers that the Providers Enquiry Line currently represents the biggest risk for fraudulently obtaining Medicare numbers. The information required for a phone enquiry is readily available to anyone who has been provided a service by a medical practice.

Another alternative for strengthening the security around phone confirmations of Medicare numbers would be to provide each practice with an Identification Number and perhaps an access PIN, similar to telephone banking arrangements. This information could be then be used to verify that the enquiry is genuine.

Access to Medicare numbers via the Providers Enquiry Line could be strengthened by having a list of authorised contacts. The AMA would expect these would be the same as delegated authorities under HPOS and that the Department of Human Services could use this list of names, ensuring no additional administrative burden for practices.

Encouraging health professionals to use HPOS for Medicare card enquiries

The best way to ensure that health professionals utilise HPOS is for it to be accessible from within practice software. This would further facilitate streamlined access to the services and resources of the Department of Human Services for health professionals.

Protecting the security of Medicare card information in the community

Building public awareness about protecting Medicare information

The AMA has supports the concept of an awareness raising campaign so that patients understand the importance of the Medicare card in accessing their Medicare entitlements and that they should not share the information on their card inappropriately.

Reminding organisations of their obligations to protect Medicare information

The AMA supports this, recognizing that it should be an ongoing focus of the Department of Human Services.

Identity requirements when access health services

Introducing new identify requirements for access to Medicare services

The AMA believes the Review should be focussed on ensuring the security of Medicare's own mechanisms, such as HPOS Patient Finder and the Provider Enquiries Line for confirming patient's eligibility for Medicare. Requiring practices to demand ID from patients does not address the alleged criminal activity that prompted this inquiry and simply appears to be an attempt to address concerns about the administration of Medicare cards, which should be a problem for Government to solve as opposed to medical practices.

It would place an additional administrative burden on practices and put in place an unnecessary barrier to care for patients. To the extent that weaknesses in the Government's administration of Medicare cards might result in a small number of patients gaining access to a Medicare funded service that they are not entitled to, this should not be allowed to overshadow the importance of timely access to medical care.

Medicare card as evidence of identity

Retaining the Medicare card as evidence of identity in the community

The AMA supports the continued use of a Medicare card as a secondary evidence of identity, noting it is issued by the Government and in such circumstances is used in conjunction with other forms of identification.