AMA Submission to Senate Standing Committee for Finance and Public Administration:

Circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web'

September 2017

Submitted to: fpa.sen@aph.gov.au

Introduction

The Australian Medical Association (AMA) welcomes the opportunity to make a submission to the Finance and Public Administration References Committee in relation to the above Inquiry.

The AMA is strongly committed to ensuring the privacy of patients, which is fundamental to the trusted relationship between doctor and patient. Doctors are strongly aware of their ethical, professional and legal duty to protect their patients' personal information.

Any response to the alleged sale of a small number of Medicare numbers on the dark web needs to be proportionate. In developing any recommendations, the Inquiry 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 favour 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.

The AMA's response to the inquiry will address the queries as per the inquiries terms of reference.

a) Any failures in security and data protection which allow this breach to occur

For the purpose of this submission the AMA will focus on PKI certificates. We understand that that a PKI site certificate can be installed on a provider's practice software or web browser, and once logged into, can be used by anyone using the software or browser.

It is not easy for either an entity or an individual to obtain a PKI certificate. Specific pieces of information are required, which in most circumstances would only be known to the applicant. Applicants must be able to verify their identity and provide declarations of compliance. It is unlikely that an applicant would apply for a PKI unless they legitimately required it, while the verification process undertaken by the Department of Human Services (DHS) should ordinarily ensure that only legitimate applicants are issued with a certificate.

The AMA understands that entities and individuals who have been issued PKI certificates have an obligation to ensure the certificates are used appropriately and to notify the DHS if their certificates are in any way compromised. The AMA is not aware if a failure to comply with this obligation created a circumstance where Medicare numbers could be obtained and ultimately sold on the 'dark web'. However, if that proves to be the case, the AMA would suggest that the complicated and confusing nature of the multiple policy and terms and conditions documents that applicants are expected to comply with may be worth addressing.

The AMA believes that the outcome of the Australian Federal Police investigation into this incidence will best inform the Committee on what failures in either security or data protection occurred in order to facilitate this criminal act.

b) Any systemic security concerns with the DHS Health Professional Online Services (HPOS) system

The AMA believes that the Provider Digital Access (PRODA) system for accessing HPOS is more secure, as it requires not only an individual user name and password but a verification code which is auto-generated and sent directly to either the mobile or email of the person whose user name and password has been entered.

The primary risk with access to HPOS, whether by PRODA or PKI, is that an unauthorised user may gain access to the system if the authenticated user leaves their machine (be it computer, mobile or tablet) unattended. The HPOS login will time out after 30 minutes of inactivity in HPOS. The opportunity for inappropriate interaction is limited by accessibility, time-out of login, any screen time-outs, or local system security measures. Consideration could be given to reducing the period until time out.

The Committee should give particular consideration to the risk of inappropriate access to Medicare numbers via the phone enquiry line. To obtain someone's Medicare number, callers need only provide the health care provider's full name, provider number, location of the practice, along with the first name, surname, date of birth and potentially the address of a person. Provider information can be obtained in most cases from an invoice or prescription. This kind of breach would most easily be undertaken by someone known to the patient, but internet and telephone 'phishing' activities can catch out the unwary.

The AMA believes that it should be relatively straightforward to address this vulnerability, without having to disable this option. It is a vital point of access for practices, particularly for those with poor or intermittent internet connections. Mechanisms, similar to those used for telephone banking, could be implemented to provide additional security. For example, providing practices with an identification number and a PIN could be used to verify the enquiry is from a genuine provider. This would also enable DHS to keep a track of the practice where the Medicare number enquiry call came from, something which they currently do not do.

(c) The implications of this breach for the roll out of the opt-out My Health Record System

The AMA does not believe this breach has any implications for the My Health Record. It is completely unrelated and the Australian Digital Health Agency has reassured the AMA that unauthorised access to a Medicare number cannot, of itself, allow unauthorised access the My Health Record of the card holder. The My Health Record has multiple layers of security and strict controls on who can access information in the record.

The AMA understands that under opt-out arrangements individual access to their My Health Record will still be password protected. This rules out the possibility that unlawful access to a Medicare card number, date of birth and address of card holder, will give access to that card holders My Health Record.

Unfortunately, media reports that have incorrectly linked the sale of Medicare card details to the security of the My Health Record. This may have undermined the confidence of both the community and doctors in the My Health Record system. Ideally this negative messaging should be countered by strong reassurance from the Australian Digital Health Agency as system operators.

d) Australian government data protection practices as compared to international best practice

This question is best answered by Government agencies and any technology providers used by the Australian Government.

e) The response to this incident from government – both ministerial and departmental

The AMA is satisfied that Government responded appropriately to reports of the alleged breach, identifying where the breach occurred in a timely fashion and also establishing an Independent Review of Health Providers' Access to Medicare Card Numbers. The review is being conducted quickly with a final report due 30 September 2017.

The only danger that the AMA sees is that a disproportionate response may be implemented, which might impact on patient access to care and impose new layers of red tape on medical practices.

f) The practices, procedures, and systems involved in collection, use, disclosure, storage, destruction and de-identification of personal Medicare information

The Office of the Australian Information Commissioner provides a freely available guide for entities in securing personal information and meeting their requirements under the *Privacy Act 1988* (Cth) (Privacy Act).

The Royal Australian College of General Practitioners (RACGP) *Standards for general practices*, 4^{the} edition, against which general practices are accredited, provides for the management and security of patient health information under Standard 4.2, Criterion 4.2.1 and 4.2.2.

The AMA supports the overarching health privacy legislation that protects the privacy of personal and sensitive information in this county. We believe it is important that the

application of general privacy laws to the health sector enhances – not hinders – the provision of quality health care. The AMA in supporting doctors has a guide to assist medical practices to understand and meet their privacy obligations.

g) Practices, procedures, and systems used for protecting personal Medicare information from misuse, interference, and loss from unauthorised access, modification or disclosure

For health care providers' see above.

h) Any related matters

Identity Requirements when Accessing Health Services

The AMA is concerned at the possible recommendation flagged in the discussion paper released by the Independent Review of Health Providers' Access to Medicare Card Numbers that new patients should be required to provide proof of identity before accessing medical care covered by Medicare. This could impact on the ability of vulnerable patients to access health services via the MBS.

Introducing a requirement that would require individuals to present proof of identity when first attending a health service could have inherently discriminatory effects on a range of patient groups, including Aboriginal and Torres Strait Islander Australians, the homeless, mentally ill and low income earners.

With regard to Indigenous Australians many are unable to obtain primary evidence of their identity, because of problems accessing a birth certificate. Anecdotal evidence suggests there may be a multitude of reasons for the inability to access a birth certificate, including: births never being registered, insufficient understanding within Indigenous communities of the importance of registering a birth, individuals being registered under a different name (as is the case for many members of the stolen generation), high fees, literacy/language difficulties, marginalisation from mainstream services, and a distrust of authorities.

People who are homeless or on very low incomes may not hold a current driver's licence or passport, nor may they have an electricity or phone bill in their name. Those escaping domestic violence situations may also not have access to identifying documentation. Patients in a distressed state mentally may also be unlikely to have any ID on them and being asked to prove their identity when in an agitated state may exacerbate their symptoms, putting them or others at risk.

The AMA believes this proposal would create an unnecessary and discriminatory barrier to medical care.