RACGP

Royal Australian College *of* General Practitioners

RACGP eHealth & Practice Systems

Submission to the Independent Review of Health Providers' Access to Medicare Card Numbers Discussion Paper.

September 2017

Healthy Profession.
Healthy Australia.

Introduction

The RACGP welcomes the opportunity to provide written comment to the Independent Review of Health Providers' Access to Medicare Card Numbers.

The RACGP is Australia's largest professional general practice organisation representing over 35,000 members working in or towards a career in general practice.

General practitioners (GPs) see approximately 85 percent of the population every year and collect, record and store comprehensive patient data[1].

The RACGP takes the issue of patient privacy and confidentiality very seriously. The news that personal Medicare data of Australians was compromised and made available for sale by a dark net trader was deeply concerning to us and we support the review's aim to improve security of patients' Medicare data without compromising healthcare provider access to Medicare information for the purpose of confirming patient Medicare eligibility.

Responses to consultation questions

1. Do patients have sufficient control and awareness of access to their Medicare card details?

Whilst we cannot speak on behalf of our patients, a government directed communications campaign, run by health care organisations, could be a useful strategy to build patient awareness of access to personal Medicare card details. This would include the circumstances in which health care professionals will access patients' Medicare information via Government systems, and the avenues available to patients to review their claiming history. In the context of this review into health providers' access to Medicare card numbers, the RACGP's view is that healthcare organisations' access levels to patient Medicare information should remain in order to be able to verify patient eligibility and provide essential services.

Further, the Australian public has a role in reducing the risk of identity theft by safeguarding information. Investment in public awareness and education campaigns on personal information protection strategies will assist in strengthening the security of Medicare information.

2. What identifying information should patients have to produce to access health services?

To reduce the risk of fraudulent use of Medicare card details, requiring patients to present another form of identification on first registering with a healthcare organisation may be a useful strategy. The introduction of such a policy should take into consideration any additional barriers to healthcare access that this might create, particularly for vulnerable patients. A clear and targeted consumer communication strategy will be important to ensure heath consumers are aware of this requirement, its purpose and are educated on the types of additional identification deemed sufficient.

The RACGP supports the Review Panel's recommendation that patients unable to produce identification can still access urgent or emergency treatment. However, practices will require further guidance on what constitutes urgent or emergency treatment and the point at which these patients requiring continuing care and treatment are required to produce identifying documentation to confirm their Medicare eligibility. How this is managed and the overarching policy to guide decision making will inform whether this is best regulated by industry bodies or a formal legal condition managed by the Department of Human Services.

3. Are the current access controls for HPOS sufficient to protect Medicare information and prevent fraudulent access?

The RACGP is satisfied with the current security protocols required to access the HPOS system.

The RACGP supports the continuation of a system where health care providers and, in particular, administrators can safely access Medicare details of patients via a system such as HPOS. Restricting access to Medicare information or increasing the complexity of access levels and therefore the time required to verify patient Medicare information could compromise the provision of essential healthcare in circumstances where patients cannot confirm evidence of eligibility. This poses a significant risk to Australia's most vulnerable people.

4. What would the impact on health professionals be if they were required to move from an individual or site level PKI certificate to a PRODA account? Would any enhancements to PRODA be required for health professionals to accept it as a replacement?

The RACGP supports any initiative that strengthens the security of the HPOS system, providing this is balanced with reasonable administrator access to patient Medicare information. The RACGP supports the move from PKI certificates to Provider Digital Access (PRODA) accounts to enhance the security of HPOS verification. However, healthcare providers and supporting organisations must have a National Authentication Service for Health (NASH) PKI certificate to access the My Health Record system and to send and receive messages securely using software that meets the requirements for secure message delivery. It is important that a PRODA-based alternative to site certificates is developed that does not increase the administrative burden of accessing HPOS or create complexity through the need for multiple authentication processes. Patient verification through practice software must still be possible.

5. If PRODA accounts and PKI certificates were to be suspended following a period of inactivity, what processes or alerts would the Department need to put in place? What would be a reasonable period of inactivity before accounts were suspended?

If PRODA accounts and PKI certificates are subject to expiry dates, users should be required to undergo a renewal process. Automatic prompts within systems could alert users of impending expiry dates. Extensive consultation will be needed with healthcare providers to establish a reasonable timeframe before an account expires and a suitable process for notification of expiry dates.

6. If delegate arrangements in HPOS were to be time limited, what processes or alerts would the Department need to put in place? What would be a reasonable period for delegate arrangements to last before they require review?

As above.

7. In what circumstances do health professionals need to make batch requests for Medicare card details through HPOS Find a Patient? Can such requests be limited to certain types of providers or health organisations? Should they be subjected to a higher level of scrutiny?

Circumstances in which batch requests for Medicare card details are necessary from a general practice are rare. The RACGP does not oppose the recommendation of the Review Panel that an upper limit is applied to the number of requests that can be made in one batch. The RACGP recommends further consultation is

undertaken to determine if placing limits on who can make batch requests imposes an additional administrative burden on healthcare organisations.

8. In what circumstances do health professionals require access to Medicare card numbers through the provider enquiries line? Could the provider enquiries line be made available in more limited circumstances?

If the online HPOS system was inaccessible, health professionals may need to obtain Medicare card numbers through the provider enquiries line. Further, Medicare information is not infallible. It may be necessary to access the provider enquiries line in the event that patient Medicare information is recorded incorrectly and therefore cannot be verified through HPOS.

As the provider enquiries line is far less secure than the online option, the RACGP supports the Review Panel's recommendation that HPOS is the default mechanism for requesting patient Medicare card numbers, and the recommendation that the provider enquiry line is available in a reduced capacity. To support practices with this change, it is important that the online security process does not place an unnecessary time burden on administrators using the HPOS system to access Medicare information.

9. Is the information available to health professionals regarding their obligations to protect Medicare card information (including the terms and conditions for accessing this information online) sufficiently clear and understood?

The RACGP supports the Review Panel's recommendation to review the PKI and PRODA terms and conditions so as users' obligations are as clear as possible in terms of their own and third party access. To complement the information already provided, a funded peer education program could further support general practices to increase the safety of Medicare information collected, used and stored.

The RACGP also provides members with various resources, including the *Computer Information Security Standards 2nd Edition*, which provides cybersecurity and privacy guidance to help GP clinics develop best practice information security policies and procedures, reducing their vulnerability to data breaches.

10. Should Medicare cards continue to be used as a form of evidence of identity?

Medicare card details are often used for general identity verification purposes. Rather than restricting provider and patient access to Medicare information for purposes relating to healthcare provision, reducing the value of Medicare details for non-medical verification purposes may reduce its vulnerability as a means of identity theft.

11. How can Government build public awareness of why it is important for individuals to protect their Medicare card information?

The Australian public have a role in reducing the risk of identity theft by safeguarding their information. Investment in public awareness and education campaigns on personal information protection strategies will assist in strengthening the security of Medicare information. Primary Health Networks (PHNs) could be most appropriate organisations to lead such a campaign and engage with the public in their local areas.

12. Do you have any other comments about the Review Panel's possible responses or any other matters relating to the Terms of Reference?

NA

Concluding comments:

As the representative body for more than 35,000 members working in or towards a career in general practice, the RACGP is deeply concerned about any issues relating to the sale and use of unauthorised Medicare data. The RACGP supports the Independent Review of Health Providers' Access to Medicare Card Numbers and welcomes any further opportunity to work with government in improving patient data safety.

References

1. National Health Performance Authority. Healthy communities: Frequent GP attenders and their use of health services in 2012–13. Sydney: NHPA, 2015.