RACGP

Royal Australian College *of* General Practitioners

RACGP eHealth & Practice Systems

RACGP Submission to the Senate Finance and Public Administration Committee regarding *Circumstances in which Australians' personal information has been compromised and made available for sale illegally on the 'dark web'*.

August 2017

Healthy Profession.
Healthy Australia.

Introduction

The RACGP welcomes the opportunity to provide a written submission to the Senate Finance and Public Administration Committee regarding the circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web'.

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 initiatives to improve the safety of Australians' Medicare information.

Responses to terms of reference

a. any failures in security and data protection which allowed this breach to occur;

The RACGP understands from media reports, that a dark net vendor exploited a vulnerability in a government system to obtain access to personal Medicare information. The RACGP is aware that the matter is being investigated by the Australian Federal Police, and that separate to this investigation, an independent review into the matter has been commissioned. The review aims to provide government with information about any system vulnerabilities and how these can be addressed. The Review Panel has released a discussion paper *Independent Review of Health Providers' Access to Medicare Card Numbers* and the RACGP supports the recommendations made by the authors of this paper. The RACGP is satisfied steps are being taken to determine which government system was infiltrated and to address any security and data protection failures.

Health care organisations across the sector, including medical, allied and dental health centres are connected to the Medicare claims and payments databases and can access patient Medicare numbers. While preventative measures can be implemented, in an interconnected world, there is a real and persistent risk of any organisation suffering either an internal or external data breach.

The RACGP produces a suite of resources to support general practices to minimise the risk of data breaches including the Computer information security standards (currently under review). General practices that implement the cybersecurity and privacy guidance provided in this document are less vulnerable to a data breach.

b. any systemic security concerns with the Department of Human Services' (DHS) Health Professional Online Services (HPOS) system;

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 could compromise the provision of essential healthcare if patients are unable to confirm evidence of eligibility. This poses a significant risk to Australia's most vulnerable people.

The RACGP supports any initiative that strengthens the security of the HPOS system, but it is important for this to be balanced with reasonable administrator access to patient Medicare information. Provider Digital Access (PRODA) is an online authentication system where a username, password and verification code are required to log in. The system is designed to provide secure access to specific government services. This solution is an alternative to Public Key Infrastructure (PKI) individual certificates, smart card or USB tokens and multiple username and password logins, which are used to access these services.

The RACGP supports the move from PKI certificates to 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. It is important that a PRODA-based alternative to site certificates is developed and patient verification through practice software is still possible.

c. the implications of this breach for the roll out of the opt-out My Health Record system;

The RACGP does not foresee significant implications for the rollout of the opt-out My Health Record system as a result of this data breach. A Medicare card number alone does not allow access to a patient's My Health Record. The authentication process for both the consumer and provider portals of the My Health Record are complex and have many layers of security.

Individuals can elect to opt-out or can set strict privacy controls, enabling full control over third party access to personal information. A clear and targeted consumer communication strategy will be important during the implementation of the opt-out My Health Record System to allay any fears of identity theft and connection with this recent data breach.

However, one scenario that does need attention is if a stolen Medicare number is used to access healthcare and information about this care, such as PBS and MBS data, is then automatically sent up to the patient's My Health Record.

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

No comment

e. the response to this incident from government – both ministerial and departmental;

The Government response to this incident was appropriate, acknowledging the seriousness of such a data breach, and commissioning an independent review into the breach to address the issues rendering patient Medicare data vulnerable. However, we understand that the Government had previously been alerted to the availability of Medicare card numbers on the dark web and it is not clear what response was taken at the time. The RACGP expects that the Government will communicate with key stakeholders about the nature of the breach and steps taken to mitigate future risk, as this information becomes available.

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

General practices, along with other healthcare organisations, require the ability to collect, use and store patient Medicare information in their practice management systems in order to undertake administrative functions relating to the Medicare Benefits Schedule (MBS). If a GP clinic believes it has experienced a data breach, the RACGP advises members to promptly report it to the Office of the Australian Information Commissioner (OAIC). The RACGP's resource *Computer and information security standards 2nd edition* (currently under review) provides cybersecurity and privacy guidance to help GP clinics develop best practice information security policies and procedures, reducing their vulnerability to data breaches. As

general practices are often small businesses with limited capacity to invest in technology and systems to support computer information security, a funded peer education program could further support general practices to increase the safety of Medicare information collected, used and stored.

g. the practices, procedures, and systems used for protecting personal Medicare information from misuse, interference, and loss from unauthorised access, modification, or disclosure;

While the design and functionality of systems, procedures and practices for protecting Medicare information are important, 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.

h. any related matters

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.

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 this inquiry into the circumstances in which Australians' personal information has been compromised and made available for sale illegally on the 'dark web' and welcomes any further opportunity to work with the 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.