RACGP

Royal Australian College *of* General Practitioners

RACGP response Consultation for the Australian Digital Health Agency Cyber Security Strategy

Healthy Profession.
Healthy Australia.

1. Introduction

The Royal Australian College of General Practitioners (RACGP) welcomes the opportunity to provide written feedback to the Australian Digital Health Agency (the Agency) Cyber Security Strategy Development consultation.

2. About the RACGP

The RACGP is Australia's largest professional general practice organisation, representing over 45,000 members working in or toward a career in general practice, including 4 out of 5 GPs in rural and remote areas.

The RACGP is responsible for:

- defining the nature and scope of the discipline
- setting the standards and curricula for training
- maintaining the standards for quality general practice
- supporting specialist general practitioners (GPs) in their pursuit of excellence in patient and community service.

This response has been informed by the RACGP Expert Committee – Practice Technology and Management (REC–PTM), which oversees and supports a program of work relating to digital health, practice management and emergency preparedness and response.

3. Cyber security current state

The RACGP provides the following comment in response to the consultation themes and questions.

3.1 Threat context

Overall, the RACGP has good awareness of changing trends and activity within the cybersecurity threat landscape and we support our members through awareness raising activities, education and resources covering:

- protection against inappropriate access to patient information, either intentional or unintentional
- business continuity to ensure practices can brings information systems back to working order when a system failure occurs
- plans for how practices can continue to function in the event of an environmental or natural disaster
- data breaches to ensures practices respond as soon as possible to minimise potential loss or corruption of information following a possible breach
- ongoing review, updates and testing of cybersecurity response plans to ensure they meet the ever change needs of general practices as small businesses with legislative obligations.

The RACGP's Information security in general practice is the key resource for our members and provides details on how to protect practice information systems from cybercrime and online threats.

The Agency should consider developing:

- a "go to resource/service" for health services in need of technical expertise and advice
- specific general practice-based advice on putting information security processes into practice
- clear explanations for clinicians and patients on how data is protected in government systems such as My Health Record.

3.2 Current state themes

Our members understand the challenges and issues, and many will have had experiences of near misses with malicious actors or data breaches caused by accidental internal activity, but there is a lack of confidence in how to respond to incidents and changing threats. Whilst GPs understand the privacy and cyber security implications when interacting with sensitive health information, as contractors, most GPs do not actively contribute to specific cybersecurity policies and measures. This is seen as being a role for practice owners and managers and other parties such as external IT contractors. The key challenges with cybersecurity in general practice are:

- who to contact once a threat is identified to either report the incident or seek advice on how to deal with the incident
- the need to balance accessibility to clinical information systems via remote access with the need for security
- how to safely integrate new digital tools for clinical care, in particular telehealth
- how to develop and promote a team-based approach to cybersecurity
- staying current with emerging threats and mitigation strategies.

Regarding services provided by the Agency / Government, our members will generally assume these are secure. They feel challenges in using these services are due to lack of integration with current workflows, data integration and a lack of easily accessible relevant information.

4 Future trends

The Agency has a key role in providing support and technical expertise to healthcare peak bodies and individual healthcare businesses to stay abreast of trends. To support privacy and cyber security the Agency could:

- continue to support the implementation of secure messaging across the whole health sector including hospitals, the allied health sector and pharmacy
- implement Active Script List roll out to all pharmacies and provide education for GPs and pharmacists about how this works
- develop generic and consistent electronic pathology and diagnostic imaging requesting

- expand the use of NASH certificates to provide a single sign on for other services such as state-based systems for real time prescription monitoring, Workcover certification, death certificate reporting, disabled parking permit applications and discount taxi service applications
- provide targeted and accredited education and training for GPs and other members of the practice team including practice managers and practice nurses
- raise awareness of the availability of existing cybersecurity services.

4. Conclusion

We look forward to working collaboratively with the Agency and other relevant stakeholders on the development of the Cyber Security Strategy.

Should you have any questions or comments regarding the RACGP's submission, please contact Ms Joanne Hereward, Program Manager Practice Technology and Management at joanne.hereward@racgp.org.au