RACGP

Royal Australian College *of* General Practitioners

# *RACGP response:*
# *National Data Security Action Plan*

**June 2022**

# Contents

## 1. Introduction

The Royal Australian College of General Practitioners (RACGP) is pleased to provide a response to the National Data Security Action Plan Discussion Paper (the Action Plan). Our response has been structured to align with the Australian Department of Home Affairs call for views.

## 2. About the RACGP

The Royal Australian College of General Practitioners (RACGP) is Australia's largest professional medical college. The RACGP sets and maintains the standards for high quality general practice in Australia and advocates on behalf of the general practice discipline. As a national peak body representing over 45,000 members working in or towards a career in general practice, our core commitment is to support Australian general practitioners (GPs) address the primary healthcare needs of the Australian population.

As an independent member-based organisation, we lead the way in facilitating continuous improvement in general practice through clinical, educational and digital advances. The RACGP is responsible for defining the nature of the discipline including setting the standards, creating the curriculum, and providing ongoing education and training. We support GPs in their pursuit of excellence in health care and community service.

This response has been prepared 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. The RACGP response

The Royal Australian College of General Practitioners (RACGP) supports, in principle, the development of the proposed National Data Security Action Plan.

The RACGP makes the following key recommendations:

- Government must ensure general practice is actively engaged and consulted on the implementation phases of the Action Plan. The RACGP should be provided with the opportunity, and funding, to provide GP representation on relevant working groups to inform proposed changes directly impacting general practice systems.
- The Action Plan should support improved interoperability and the secure and seamless transfer of information between patients, their GP and others involved in their healthcare in order to achieve a standardised data security approach across the health sector.
- The Action Plan should recognise that increasing the data security capability of the general practice workforce is complex and takes time and requires planning, financial investment, and must be supported by education and training to increase uptake and adoption.

- The Action Plan should recognise the health sector is particularly vulnerable to data breaches, due to the high volume and value of individual health data. It must offer a tailored, targeted and supportive approach to ensure health data is prioritised for enhanced data security across the nation, including data contained within general practice.
- Standards must be prioritised for delivery to ensure consistency and compatibility and should be developed through a collaboration of users, experts in clinical informatics and vendors of clinical information systems. The RACGP is a leader in standards development in general practice and well positioned to lead work in this area.
- The Action Plan must consider health equity issues and ensure all Australians have access to knowledge and training on data security that is targeted to their specific needs as required.
- The Action Plan must support and protect Aboriginal and Torres Strait Islander peoples fundamental right to data sovereignty and ensure Aboriginal and Torres Strait Islander people inform the development of the strategy through an ongoing Indigenous Advisory Committee.

## 4. Response to survey questions

**Data localisation – Getting the balance right**

*4.1 What do you consider are some of the international barriers to data security uplift?*

We have seen great benefits to cross-border data flows, such as leveraging critical COVID-19 research data and resources, leading to the rapid development of knowledge, diagnostics, and vaccines. Despite the potential opportunities that leveraging shared information internationally has for global health, there is the need for balance to ensure sensitive national data remains secure and safe and patient privacy is protected and the security and integrity of records like My Health Record are not undermined.

While Australia maintains an influential and trusted international reputation, it is not immune to the risks of malicious actors. Mitigating this risk may inhibit potentially beneficial cross-border data flows with less secure international partners. The fragmented approach internationally to data security laws and data storage approaches provides a challenging environment for a data security uplift, as it may restrict international data flow and thus the global economy.

Therefore, the RACGP believes it critical for this data security uplift to be considered and there may be an ongoing need to store, transfer, process and handle certain data sets within Australia.

*4.2 How can Australian Government guidance best align with international data protection and security frameworks? Are there any existing frameworks that you think would be applicable to Australia's practices (e.g. the European Union's General Data Protection Regulation)?*

The RACGP is concerned that protecting healthcare data is not emphasised in the Action Plan, as it is often subject to breaches. The recent report from the Office of the Australian Information Commissioner (OAIC) clearly shows the health sector as the top industry to notify data breach reports[i].

GPs are the backbone of Australian healthcare, providing more than 170 million services each year.[ii] A thriving, accessible and high-quality general practice sector is vital to the health of the nation, and its data security must be prioritised. General practice predominantly stores its patient and business data locally, mostly due to the slow uptake of cloud based clinical information systems. Given the substantial amount and value of data in general practice, a tailored, targeted supportive approach is required.

It is critical the Australian Government seeks to align with and exceed the highest standards in international data protection and security frameworks, with robust laws to ensure the protection and privacy of sensitive patient information contained on Australian Commonwealth systems such as My Health Record. All existing frameworks should be considered and evaluated in collaboration with international partners and representatives from the business and health sector where appropriate to determine recommendations and future guidance as relevant to small business such as general practice.

*4.3 What additional guidance or support from Government would assist you to meet a principles-informed approach to data security? How would this be delivered best to you?*

The RACGP supports the principles informed approach described in the Action Plan. In order to meet a principles informed approach to data security, the Government must provide a consistent, proportionate and considered approach to data security, both in policy and legislation. Data security across Federal, state and territory governments and industry need to be consistent and well communicated as part of a national Action Plan. Data security cannot be divisible from the data governance, and data governance must be clear on ownership of the data and the delegation of responsibility for the production, curation, ownership at stratified levels, storage and secondary uses.

One of the challenges for general practice are the limitations in patient management systems which require practices to deploy third-party solutions. These solutions include, but are not limited to, data analytics, communications, online bookings and clinical decision support. There are currently no data governance standards to ensure these systems handle patient and provider information securely. This means practices may share responsibility for data beaches caused by inadequate data security from third party vendors, creating an additional layer of risk as most of these solutions require data to leave the practice. This process also makes the data increasingly vulnerable to malicious actors. It is critical the Action Plan contains clear standards and outlines responsibilities that are developed in consultation with general practice, including engagement with the medical software industry.

A strong governance framework along with robust data policy is required, especially in relation to data linkage. To ensure its success, strong general practice representation on any data governance committee or advisory group relating to the Action Plan is essential. This will ensure data security guidance is fit for purpose and supports the increased connectivity across the health sector more broadly. Government must also develop secure data linkage systems to allow optimum use of data for population health research and critical data exchange across the health system.

GPs, healthcare professionals and vendors must be supported to participate in data security initiatives, including via targeted education and financial incentives. Incentives need to be considered alongside building sustainable business models to support participation in the Action Plan.

Providers of data and healthcare consumers need to understand where their data is held along with how their data may be used and linked. A robust de-identification process must be put in place, with strict security and accessibility protocols in place. This will ensure those sharing data have confidence in doing so, knowing patient's health information is secure and protected. Governance needs to be robust to protect the public interest and to ensure the sharing and use of data does not cause any unintended harms.

In ensuring the health workforce is data-enabled, education and training delivered to general practices should be fit for purpose and specific to general practice. Additionally, those who supply the data, including general practice, should share in the value generated by this and have access to data for research and quality improvement activities. The RACGP would welcome working with the Australian Department of Home Affairs on this.

The RACGP is well positioned to provide comment and advice on what is feasible and useful for general practice and on how the proposed Action Plan will impact GPs and their practice teams. We request that the RACGP is provided with an ongoing support to provide GP representation on relevant working groups.

*4.4 How could Australian legislative and policy measures relating to data security be streamlined to better align with your obligations in international jurisdictions? Does variation in international approaches create hurdles to your effective participation in the global market?*

Not applicable.

*a. What obligations are you most commonly subjected to from international jurisdictions?*

Not applicable.

*4.5 Does Australia need an explicit approach to data localisation?*

The RACGP supports an explicit approach to data localisation, particularly in regard to ensuring sensitive patient information is not stored or handled offshore. The Australian Commonwealth legislation for securing patient data on My Health Record currently ensures robust data security and control of sensitive patient information.

It is critical for consumer confidence that enhanced security mechanisms and measures are in place, such as data localisation of individual My Health Records. Australians expect that their personal information will be handled with care when they choose to engage with a product or service and are more likely to entrust their data to organisations that have demonstrated effective privacy management. [iii] Therefore, individuals must be put at the centre of the Action Plan, with patients expecting and trusting the Australian Government has an explicit approach to ensuring their data is stored safely and locally.

**Government's role – Federal, State and Territory and Municipal Government uplift**

*4.6 How can data security policy be better harmonised across all jurisdictions? What are the key differences between jurisdictions that would impact the ability to implement standardised policies/are there any areas of policy that could not be standardised? If yes, why?*

The RACGP supports in principle harmonisation of data security policies but acknowledges challenges relating to the current lack of interoperability across clinical information systems.

The RACGP believes the key role of standards is to create consistency and compatibility. The current healthcare IT systems use different coding and terminology across fragmented systems making it difficult to transfer, compare and analyse data, presenting a key barrier to effective data security, exchange and interoperability. These issues must be resolved to create the foundation for national standardised data security and interoperability policies and standards to be implemented across the healthcare sector. These must include principles based policies where appropriate collection, storage and use of health data (including for research) is founded on consumer-supported principles which ensure robust privacy and security of individual information.

*4.7 Who is currently responsible for ensuring consistent and commensurate uplift of local government data security and how can this be strengthened? Do you think responsibilities should be shared across more bodies, or shifted elsewhere entirely?*

The RACGP believes it is essential data security measures and approaches to secure general practice data are developed in consultation with peak health bodies and persons that understand general practice including GP experts, researchers and informaticians. This will ensure consistent measures that align with general practice workflow and clinical information systems, including secure patient data transfer to My Health Record, supporting the overarching responsibilities of the Australian Government for ongoing management.

*4.8 What are the main challenges currently faced by industry as a result of inconsistent data security practices between all levels of Government, including municipal governments?*

As mentioned in response 4.6, there is a current lack of standardisation and interoperability between different medical software systems, including the transfer of patient data to Australian Commonwealth My Health Records.

Data linkage, extraction and analysis is often not a simple process, requiring third party software, mapping between different codes and manual handling of data. Despite well intentioned data security practices, the RACGP is concerned that each of these different systems provides opportunity for data security breaches to occur. This makes patient data particularly vulnerable to malicious actors seeking to gain valuable information. Subsequently, this creates patient concerns around the security of data.

The RACGP believe providing consistent data security not only between all levels of Government, but also across general practice and the health care sector more broadly is critical, and dependent on standardisation and interoperability of information systems.

**Clarity and empowerment for business – Data centres and supply chains**

*4.9 What steps could your business take to better understand the value of the data they process and store? Do businesses have sufficient awareness of their data security obligations?*

General practice is a leader in the use of technology to deliver healthcare. Approximately 96% of general practices collect, record and store comprehensive patient data electronically. This has enabled general practice to continuously improve the quality and efficiency of care delivered to patients. General practice understands they have ethical requirements to ensure the security of their patients' data.

The RACGP produces a number of resources in tis area to support GPs, including *Information security in general practice.*

The RACGP has also produced the Minimum requirements for general practice clinical information systems to improve usability report, which identifies and details a number of key clinical information system (CIS) functions and roles and provides recommendations focused on improving usability in the collection, management, use and sharing of information. We are, therefore, well positioned to support the development of a detailed minimum set of GP CIS standards. This would support improved awareness of data security obligations.

Similarly, to build trust in the community and the health sector that the data collected is secure and appropriately managed, the RACGP's Guiding principles for managing requests for the secondary use of de-identified general practice data provides advice in his area.

*4.10 How can the Australian Government further support your business to understand the value of data and uplift your data security posture?*

The provision of contemporary healthcare sees patients interacting with multiple healthcare professionals and organisations across several locations. Efficient communication between all parties is critical to ensure the delivery of high quality, effective and safe healthcare.

General practice has been an early adopter of new technology, including electronic clinical, administrative and communication systems. For example, secure messaging has enabled general practice to increase the quality, safety and efficiency of care provide, enabling general practices to seamlessly receive, review and incorporate health information and data from other sources into their existing local health records efficiently. General practice understands the value of data, acknowledging its use must happen in a way that supports patient confidentiality, quality clinical handover and effective continuity of care. For example, high quality patient care depends on a GPs timely access to safe, secure, and accurate data and the ability to securely receive and send clinical information across a patient's multidisciplinary team.

Health data, including the curation of continuous and detailed patient records by GPs, must be acknowledged in the Action Plan for its immense value and demonstrated benefit to public health and planning. It is vital to ensure GPs are included in all levels of governance, owing to the large part they play in contributing to public heath data. General practice must be supported to continue this valuable work with clearly defined ownership of the data and delegations of responsibility for the production, curation, ownership at stratified levels, storage and secondary uses.

The Australian Government has a key role in providing support and technical expertise to healthcare peak bodies and individual healthcare businesses to stay abreast of trends. The RACGP believes that uplifting the security levels of general practice must be supported by a clear set of standards, that are well communicated and strengthened by training on any new data security measures. The Australian Government needs to ensure GPs and their practice teams are renumerated for their time to complete additional and ongoing training, as required, along with funding critical data security software across the health sector.

*4.11 Does your business appropriately consider data security risks in their supply chains? Is there sufficient public information provided by Government to help your business identify these risks?*

The RACGP believes in order to enable the safe and successful collection, collation and use of health data and information in general practice, and across their supply chains, it is critical the Government communicates regularly with peak health bodies and general practice on new data security risks. The Government must also support general practice with training and education required on any new data security approaches in a timely manner, including funding and remuneration for their time to participate in these activities.

Data security must be also considered across various stratified levels of risk, such as the sanctioned and assumed use of the intellectual property that is a GP curated medical record. It may be of particular value to other health sectors, and therefore its ownership and purpose of use must be clearly defined to ensure patient information serves the purpose it was intended, serving the best interests of the patient.

*4.12 Should there be overarching guidance on securing data for businesses of all sizes, or is it important to provide guidance based on a company's size? For example, a 'size' threshold).*

The RACGP is concerned about the standardisation of data security measures for business of all sizes. General practice data is incredibly diverse and standardising data security is unlikely to meet the needs of general practice and patient-centred healthcare. Additionally, rural and remote general practices tend to be smaller with limited access to technology solutions and expertise. This may result in challenges complying with the same standards required of larger companies. Therefore, a one size fits all solution is likely to lead to the very significant worsening of healthcare under servicing in rural and remote locations.

These challenges must be considered when creating overarching guidance, in consultation with general practice and the health care sector to determine an approach that works for all health care organisations and business across the health sector.

*4.13 Are there any limiting factors that would prevent Australian industry and businesses from effectively implementing an enhanced data security regime?*

The varied clinical record systems accessed and used by general practice create a diverse supply chain of data. Secure message delivery systems have been developed to support the safe and effective transfer of sensitive health information that mitigate the risks of communicating via mail, fax, and email. These systems are critical because, for example, delays caused by communicating between hospitals and general practice via ordinary mail can result in patient harm and even death.

More than 90% of general practices have access to secure messaging systems and most other specialists and healthcare organisations have secure messaging capability. However, these systems are widely underutilised, especially for outbound communications. This is largely due to a lack of standardisation, incentive, and awareness of the potential benefits of secure messaging systems.

While some jurisdictions have implemented secure message services to enable the sending of discharge summaries from hospitals to general practices, a significant proportion of health services and government agencies communicating with general practice do not use electronic communication systems which are compatible with those existing in general practice. As a result, many health professionals and organisations continue to use mail and fax. There are clear advantages for the use secure messaging across the health sector more broadly, and the RACGP has long advocated for interoperability between clinical information systems and messaging systems to enable widespread adoption of secure message delivery. The RACGP recommends establishing clear regulations to drive the necessary changes required for widespread adoption of interoperability across the health sector.

**Empowering and educating citizens and consumers (the community)**

*4.14 Does the Australian Government currently have sufficient public information for consumers and citizens on data security best practice? How can we make that information more easily accessible, usable and understandable?*

The RACGP supports strengthened privacy protections for individuals, particularly relating to online platforms and digitised service delivery as mentioned in the Action Plan. However, there is a lack of discussion on how funding and education will support awareness of these initiatives and published guidance along with a detailed approach on implementation and adoption.

While biometric data used in face recognition to verify peoples identify is acknowledged in the Action Plan, it is also critical to discuss that healthcare data extends beyond identity to include things like prescriptions, billing, and insurance, which may also invite fraudulent activity if not securely handled.

There is a lack of discussion regarding Aboriginal and Torres Strait Islander people and their fundamental right to data sovereignty. Aboriginal and Torres Strait Islander peoples could inform the development of the strategy through an ongoing Indigenous Advisory Committee.

There is also no mention of targeted actions to support people (both consumers and health professionals) who are not digitally capable. Whilst the Australian health care system is considered one of the world's best, it is also considered one of the worst in terms of health equity[iv]. Equity, as defined by the World Health Organization is "the absence of avoidable, unfair or remedial differences amongst groups of people, whether those groups are defined socially, economically, demographically or by means of stratification".

Data security in healthcare needs to transcend the boundaries of language, location, and behaviour. Australia has a richly diverse and multicultural population and many patients seeking healthcare from culturally and linguistically diverse backgrounds may not be able to receive optimal care via digital health. Data security and technologies must support culturally and linguistically diverse populations to access and store to their personal health information in an interpretable format.

Technologies should aim to improve access for all populations, particularly those most at risk of poor health outcomes, to receive high quality and timely healthcare from their usual GP and broader health care teams, and this must also consider equitable communication and access to the required knowledge and technology to ensure their data remains safe and secure.

*4.15 Should there be enhanced accountability mechanisms for government agencies and industry in the event of data breaches? How else could governments and industry improve public trust?*

The RACGP supports prompt, open and transparent communication with consumers to notify and support them in the event of data breaches. Clear policies need to be made available to consumers 'to enable Australians to engage with confidence online, governments, businesses and

individuals need to know and trust that their data is secure', including consumer trust in critical health services such as telehealth and My Health Record.

We also recommend prioritising understanding and knowledge in the community about where when, how and why their data is being collected, stored, and accessed to improve public trust. This must also include communication on how people will be notified in the event of a data breach.

Careful planning, ongoing evaluation, appropriate consultation, and appropriate resourcing will be required to improve public trust. Considered planning and development phases that prioritise meaningful contribution of consumers, including a focus on secure health data handling, will greatly improve the opportunity for successful implementation.

## 4 Conclusion

Australians see their GP more than any other health professional, with almost 85% seeing a GP at least once each year. GPs are highly trained generalist medical specialists providing the interface between the patient and the broader healthcare system.

For a National Data Security Action Plan to be successful, there must also be greater interoperability across clinical information systems along with support, infrastructure, and training for general practices. For example, support to implement or update health data security systems and to engage in education on new data security approaches and risks. System integration is critical to standardised data security, but this cannot be readily implemented by many facilities due to a lack of infrastructure, knowledge and funds.

The RACGP urges government to partner with us on both the planning and implementation phases of the Action Plan to ensure the role of GPs, as the coordinators of healthcare, is not adversely impacted by data security guidance that are administratively burdensome and do not fit with clinical workflows and software.

We look forward to working collaboratively with the Australian Department of Home Affairs and other stakeholders on the National Data Security Action Plan.

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

**References**

[i] Australian Government Office of the Australian Information Commissioner: Notifiable Data Breaches Report – July – December 2021 https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021 [Accessed 02 June 2021]

[ii] Department of Health. Annual Medicare statistics: Financial year 1984–85 to 2020–21. Canberra: DoH, 2021.

[iii] Australian Government Office of the Australian Information Commissioner: Focus on accountability to prevent data breachesm 2022 https://www.oaic.gov.au/updates/news-and-media/focus-on-accountability-to-prevent-data-breaches [Accessed 02 June 2021]

[iv] The Commonwealth Fund. Mirror, mirror 2017: International comparison reflects flaws and opportunities for better U.S. health care. New York: The Commonwealth Fund, 2017. Available at www. commonwealthfund.org/publications/fund-reports/2017/ jul/mirror-mirror-2017-international-comparison-reflectsflaws-and [Accessed 02 June 2021]