



Our reference: D2017/000366

Mr Tim Kelsey
Chief Executive Officer
Australian Digital Health Agency
Level 25, 56 Pitt Street
Sydney NSW 2000

Via email: CEO@digitalhealth.gov.au

Dear Mr Kelsey

OAIC submission on the development of a National Digital Health Strategy

Thank you for the opportunity to contribute to the development of Australia's National Digital Health Strategy (the Strategy).

Over the last six years, my Office has been the independent regulator of the privacy aspects of the Healthcare Identifiers service and, more recently, of the My Health Record system – two of the cornerstones of Australia's digital health ecosystem. During this time, we have worked with the Department of Health, the former National eHealth Transition Authority and now the Australian Digital Health Agency (ADHA) to promote and ensure that privacy considerations are prioritised and form an integral part of Australia's digital health policy.¹

I appreciate the ADHA's commitment to co-producing a national strategy for digital health and its role in supporting digital innovation. I agree that digital innovation in the health sector has the power to improve health outcomes for Australians and I am supportive of initiatives that seek to maximise and enhance the use of data in the public interest. However, as digital health initiatives necessarily involve the management of large amounts of sensitive health information, privacy must be a central consideration.

Good privacy practice and governance are increasingly recognised as essential elements for the success of new data-related activities. Ensuring that privacy concerns are meaningfully addressed in the design of policies and systems from the outset means that community expectations are more likely to be met. This can help establish a social licence for using and

¹ The OAIC has a Memorandum of Understanding (MOU) relationship with the ADHA to provide dedicated privacy-related services under the *Privacy Act 1988*, the *My Health Records Act 2012* and the *Healthcare Identifiers Act 2010*. The MOU sets out a program of work including compliance and enforcement activities, providing privacy-related advice and developing guidance and training materials for internal and external stakeholders.

sharing data in innovative and publicly beneficial ways, such as to provide more personalised healthcare, enable individuals to make better-informed choices, and facilitate the development of new treatments.

I provide some further comments in this regard below.

Community expectations and public support for digital health initiatives

The ADHA is to be commended for actively engaging with government stakeholders, the health and technology industry, and the broader community in developing this Strategy. As recognised in the Strategy's discussion paper, comprehensive and meaningful consultation is fundamental to ensuring that the Strategy meets community needs and expectations. From a privacy perspective, this is particularly important in order to ensure that any new and existing digital health initiatives use and share health data in ways that the community believes are valuable and reasonable.²

When it comes to the collection, use and sharing of data by government agencies, the landscape is rapidly changing.³ Personal information is often collected compulsorily by government in exchange for access to payments and services. However, technological developments and improvements in data analytic capabilities mean that data can now be used in ways that were not envisaged just 10 years ago. This is particularly relevant in the digital health context where the linkage, aggregation and sharing of health data can lead to significant new insights, more efficiently (and potentially more accurately) than ever before. In this respect, where data is entrusted to government agencies, and derived from personal information collected on a mandatory basis, it should be respected, protected and handled in a way that is commensurate with broader community expectations.

Additionally, for many people, health data is very personal and many people are reluctant to share it – even in a de-identified form. Public support for digital health initiatives will therefore depend on assurances that privacy will be respected and the level of control individuals are able to exert over any uses of their data.

It is the experience of my Office, and research has shown, that individuals are more likely to allow their data to be shared if they have the ability to choose the conditions under which it is shared.⁴ Government and business are increasingly recognising that providing individuals with control over how their data is used is a prerequisite for effective data sharing. For example, one of the draft findings in the Productivity Commission's recent draft report, *Data Availability and Use*, is that 'individuals expect to remain in control of who data on them is

² My Office is planning to further explore community expectations in relation to the handling of personal information, including some of the issues surrounding the types of data that individuals see value in being used and shared, in our 2017 Community Attitudes to Privacy survey.

³ For an overview of current discussions and the key issues relating to the use and availability of government and privately-held data, see the Productivity Commission's draft report, <http://www.pc.gov.au/inquiries/current/data-access/draft>

⁴ See, eg, Moore, D and Niemi, N (June 2016), *The Sharing of Personal Health Data – A Review of the Literature*, p. 5.

shared with.⁵ It is encouraging to see that the ADHA's discussion paper also notes that the Strategy will focus, among other things, on empowering people 'to have greater control and better access to information.'

It is also important to recognise that people's concerns about their personal information are often granular. For example, individuals may be apprehensive about specific pieces of health information being collected or shared rather than have a blanket concern about all of their health information.⁶ An effective and meaningful consultation process will be an open conversation that allows the ADHA to gauge these concerns and respond to them accordingly. I encourage the ADHA to continue proactively consulting with the public and the health and technology sector on specific proposals, including after the Strategy has been finalised.

Establishing a social licence for digital health initiatives

The importance of social licence has become clear in recent years. As the New Zealand Data Futures Partnership noted, '[w]hen people trust that their data will be used as they have agreed, and accept that enough value will be created, they are more likely to be comfortable with its use. This acceptance is referred to as a social licence'.⁷ Essentially, this term encapsulates how transparency and a sense of trust can help entities to use and share personal information in ways that fulfil their own objectives, as well as those of affected individuals.

Effective and meaningful consultation is one way that trust can be established between the community and government, leading to the development of a social licence. A social licence will also be established more readily if the community has a clear understanding of what is being proposed, and believes that any new uses of health data are reasonable and proportionate, having regard to the anticipated benefits.

More broadly, many individuals may not support their data being used for purposes which they see as having no clear personal (or public) benefit. This will be the case even where legislative authority to use data in certain ways exists. For example, the *My Health Records Act 2012* contains provisions that authorise the secondary uses of data in an individual's My Health Record for specific purposes. However, many individuals may not be aware of this (or support such uses). An effective consultation process and transparent analysis of risks and mitigation strategies⁸ for new uses of My Health Record data will help to establish a social licence.

⁵ Draft finding 5.3, Productivity Commission's draft report, <http://www.pc.gov.au/inquiries/current/data-access/draft>

⁶ Access controls in the My Health Record system allow individuals to restrict access to specific documents in their My Health Record. This is one feature of the system which recognises the granularity of individual's concerns when it comes to specific pieces of health information or documents.

⁷ *Data Futures Partnership*, 'What is Social Licence?', <http://datafutures.co.nz/our-work-2/talking-to-new-zealanders/social-licence/>, accessed 17 January 2017.

⁸ Privacy impact assessments (PIAs) are an essential and useful tool in mapping and mitigating a project's privacy impact and risks. PIAs can help to develop community trust in a project's intent and thereby work towards creating a social licence.

In summary, I reiterate that the success of the National Digital Health Strategy will depend largely on transparency and establishing trust as to how personal health data will be used, strong community support for new health data activities, and the ability of individuals to have control over how their data will be used.

I would be pleased to review a copy of the Strategy once the draft has been developed, and look forward to continuing to work with the ADHA on digital health initiatives into the future. If you have any questions, please contact Melanie Drayton, Assistant Commissioner, Regulation and Strategy Branch, on (02) 9284 9812 or via email Melanie.Drayton@oaic.gov.au.

Yours sincerely

A handwritten signature in black ink that reads "Timothy Pilgrim". The signature is written in a cursive style with a large, sweeping initial 'T'.

Timothy Pilgrim PSM
Australian Information Commissioner
Australian Privacy Commissioner

25 January 2017