Australian Government
Australian Digital Health Agency

Digital Identity Bill and Digital Identity Rules
Australian Digital Health Agency Submission

10 October 2023
Approved for external information

Introduction

The Australian Digital Health Agency (the Agency) thanks the Department of Finance for the opportunity to provide feedback on the draft Digital ID Bill and Digital ID Rules. The Agency's feedback on the draft Digital ID Accreditation Rules will be provided at a later date, noting there is additional time for input on the rules.

The Agency's vision is a healthier future for Australians through connected healthcare. Funded by the Commonwealth and the States and Territories in recognition that digital health must be a national enterprise, the Agency plays a key role in connecting Australians to a modern healthcare system that ensures they can access the care they need, when and where they need it.

The Agency was established by the *Public Governance, Performance and Accountability (Establishing Digital Health Agency) Rule 2016* and performs the role of System Operator for the purposes of the *My Health Records Act 2012*. The Agency also has data and digital specific responsibilities under other legislation including the *Privacy Act 1988* and the *Healthcare Identifiers Act 2010*.

Digital identity that supports the healthcare system represents a significant opportunity in supporting the provision of the right information with the right individual at the point of care, improving safety for patients and increasing efficiency for healthcare providers. Health sector engagement in the digital identity discussion is important to understand the likely impact of any changes from the reforms to digital identity on key digital health infrastructure, products and services including the My Health Record system,[1] ePrescribing and Provider Connect Australia.[2] This understanding will enable the Department of Health and Aged Care and the Agency to build on digital health modernisation work and will allow for forward planning and future proofing to support the national digital and data reform agenda.

Digital identity can also provide for a more connected healthcare delivery service, driving better health outcomes, easing pressure across the health workforce and improving the sustainability of the health system. There are benefits and implications for integration of digital identity across the entire health ecosystem for healthcare professionals and consumers accessing primary care, acute tertiary healthcare, aged care, allied health, disability support services, mental health services and more. This represents a significant opportunity to use and drive digital identity services, via federal and jurisdictional systems that are used to deliver healthcare, and could be supported within the proposed federated model.

[1] The national electronic health record system, providing consumers and their healthcare providers access to key health information when and where it is needed. More information is available at digitalhealth.gov.au/initiatives-and-programs/my-health-record.
[2] A national service that allows healthcare providers to update their business information in one place, reducing duplication and streamlining notifications. More information is available at digitalhealth.gov.au/healthcare-providers/initiatives-and-programs/provider-connect-australia.

On a broader scale, with the healthcare industry continuing to be one of the most targeted industries by cybercriminals in Australia, the importance of a secure digital identity system that can be used seamlessly in the healthcare system, and with digital health infrastructure, cannot be under emphasised.

In terms of the programs currently operated by the Agency, digital identity is in limited use. Consumers can use their myGovID to access their My Health Record through myGov (if it has already been linked), and healthcare providers use PRODA (Provider Digital Access) to access Provider Connect Australia and the My Health Record system (only through the National Provider Portal). Digital identity offers a range of opportunities to improve the way consumers and healthcare providers interact with the My Health Record system, ePrescribing and other digital health programs and services.

This submission is limited to responding to the questions posed in *Your guide to the Digital ID legislation and Digital ID Rules* (the Guide). It also covers additional considerations that may apply to the digital health domain. It does not cover questions or considerations outside of this domain.

If you have any queries or require further information, please do not hesitate to contact Jessica Carew, Branch Manager, Strategy and Policy, [redacted]

Response to questions

Q1: What other types of Digital ID service should be included in the legislation, either now or in future?

The current scope of digital identity is focused on individuals as consumers of services. In the health sector, the ability for individual healthcare professionals to use digital identity services offers the potential to enhance the existing authentication approaches to streamline access to systems that inform patient care. It is common for individuals within the healthcare workforce to be engaged to deliver care for multiple healthcare provider organisations. For example, a specialist with a private practice that also sees patients in public and/or private hospitals.

In the health sector the identity of an organisation can be just as important, such as in system-to-system exchanges. An example of this is the National Authentication Service for Health which identifies a healthcare organisation for transactions and interactions with government and non-government services and entities.

Q5: Are the maximum penalties for failure to meet accreditation requirements sufficient to deter accredited entities from not meeting their obligations? If not, what maximum penalties would be an appropriate deterrent?

The Agency considers the penalties reasonable but recognises the importance for the regulator to have a range of remedial actions so that it can respond proportionately to an entity's failure to meet its obligations depending on the degree to which an entity's behaviour was careless or deliberate.

Reputational damage can also be a deterrent so some degree of transparency about an entity's failure may be warranted.

Q7: Is the rule making power to allow disclosure of biometric information to enable sharing of verifiable credentials (under specified circumstances) an appropriate exception to the restriction on disclosure of biometric information?

The Agency considers the use of biometric information may provide a better consumer and user experience, provided there are suitable controls imposed to manage risk relating to the use of biometrics.

Q9: What is the appropriate age at which a young person should be able to create their Digital ID? What factors should be considered?

The My Health Record system provides that, from the age of 14, a consumer is responsible for their own My Health Record. This ensures the young person can decide what health information is available in their My Health Record and who can access it. It is their choice to manage it themselves or have someone else manage it for them. Being able to obtain and use a digital identity would support these young people in gaining access to and managing their My Health Record, and in delegating its management to another person.

The Agency notes that this aligns with Medicare arrangements where information about a young person who turns 14 is no longer accessible by parents or guardians without the young person's permission.

Consideration should be given to ensuring that those with limited identity documentation, potentially including those under the age of 18, are able to obtain adequate access to services using accredited digital identity providers.

Q10: What other steps could the Government consider taking to ensure the AGDIS is ready for use by private sector relying parties and accredited entities?

Most healthcare services in Australia outside of public hospitals are operated by the private sector. In particular, diagnostic services such as pathology and diagnostic imaging are mostly private. You may wish to consider piloting the use of digital identity with a limited number of nationally significant private healthcare sector relying parties ahead of the phase 3 rollout to allow the wider private sector rollout to benefit from lessons learned.

Q11: What factors should the responsible Minister consider prior to deciding to approve the AGDIS expanding into another phase?

The Minister should not only consider the success and lessons learned from each phase but the demand, through new and emerging use cases, for the next phase. The Agency notes that a slow or delayed rollout of later phases could undermine benefits realisation and adversely affect participation rates.

Q12: How would phasing the rollout of the ADGIS affect the wider Digital ID services market in Australia?

A phased rollout will benefit the wider digital identity services market in Australia if it provides a roadmap of what changes comprise each phase and when it is intended to be delivered. This will help industry confidently plan for accreditation or participation.

Q16: Are the protections for participants in the AGDIS appropriate, or are any additional protections needed?

The Agency considers the protections are appropriate.

It is expected that, as the operator of numerous government digital health services, the Agency would seek to become a relying party and participate in AGDIS given the importance of identity verification in digital health services.

The Agency will consider whether it could provide value as an attribute provider.

Q17: Noting the pace of technological change and the need for Digital IDs to stay protected by the latest developments, how can Data Standards provide an appropriate balance between certainty for accredited entities while maintaining currency?

The misuse of a digital identity in the health sector could cause significant damage so it is critical that the system have sufficient agility to respond quickly to emerging security risks.

The legislation should be technologically neutral to ensure the system has the flexibility to move to other standards or enhancements as they emerge.

The Agency would be happy to discuss how it has approached this balancing of currency with certainty.

Q18: What would be an appropriate model for the Australian Digital ID Standards Chair and are there lessons that can be learned from the Consumer Data Right model?

The Agency agrees that that the lessons learned from the CDR model should be examined. It would be valuable to understand whether the open and consultative nature of the CDR's Data Standards Board has been effective in maintaining a robust security profile and providing assurance to participants.

Additional considerations

The Agency has considered the specific elements of the proposed Digital ID Bill and Digital ID Rules from the perspective of the use within digital health systems.

- The Agency will need to understand the detailed operational requirements associated with the provision of digital identity services, in terms of the resourcing and funding required to update national digital health infrastructure and other systems to be able to use digital identity services to authenticate users. This will inform the Agency's work in developing an overall vision and strategy for digital health authentication and supporting the development of a more interoperable health system.
- Flexibility of the legislative framework is important for innovation. It may be worth noting that reviews of the *Healthcare Identifiers Act 2010* and *My Health Records Act 2012*, both of which have identity verification at their core, found that the complexity of the legislation inhibits innovation.
- The Agency notes that Medicare cards have been raised as a potential form of attribute, but they are not intended for such a purpose. Healthcare identifiers provide the opportunity for a better foundational link since they were established specifically for the purpose of uniquely identifying individuals for healthcare purposes and are available to individuals who cannot access Medicare. This opportunity could be realised through stronger links between digital identity reform and the Healthcare Identifiers Service from a legislation and systems perspectives, including in the context of the Healthcare Identifier Act reforms. Wider use of healthcare identifiers is critical to supporting the interoperability agenda to support the sharing of health information with Australians and their healthcare providers. Understanding the possible impact of digital identity reform on healthcare identifiers and identifying future opportunities to support use of healthcare identifiers in these discussions is vital to support their broader use.
- It may be appropriate to have certain identification attributes specific to the health sector which would not be appropriate for use by non-health entities, such as healthcare identifiers.
- The Agency uses PRODA for the My Health Record system and Provider Connect Australia. PRODA is not compliant with the digital identity framework so there will need to be consideration of whether PRODA remains an option for healthcare providers.

Publication date: 10 October 2023

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000 digitalhealth.gov.au
Telephone 1300 901 001 or email help@digitalhealth.gov.au

Acknowledgements
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.