

Feedback in response to Australia’s Primary Health Care 10 Year Plan, Primary Health
Reform Steering Group.

Australian Privacy Foundation

3 November 2021

About the Australian Privacy Foundation and this feedback

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. Information about the APF appears at the end of this submission. We welcome this opportunity to provide a response to the Primary Health Reform Steering Group’s consultation about the proposed 10 Year Plan (the Plan).¹

Aim

The aim of this response is to support the Primary Health Reform Steering Group’s success in devising a useful 10 year plan, which will prove to be in everyone’s best interests.

Summary

1. Implementing an Application Programming Interface (API) to connect aggregated data is inherently risky.² The Plan needs to specify that organisations, government agencies or departments aggregating sensitive health data must commit to expanding and refreshing ongoing administrative controls of well understood risks and regular audits of these controls.³
2. The Plan must embody active consent mechanisms in Voluntary Patient Registration (VPR) mechanisms, such as electronic or oral statement. Silence, pre-ticked boxes or inactivity should not constitute a valid consent.
3. The Plan needs to remain “opt in”, relying on VPR, rather than evolving into an “opt out” system, as has the My Health Record (MHR).⁴
4. A proposed direct right of action for privacy breaches suggests professionally recognised, independent, privacy and security experts must be specified in the Plan.⁵ This is good practice in any case.
5. Results from the current Office of the Australian Information Commissioner’s (OAIC’s) MHR GP privacy assessment must inform security and privacy mechanisms embedded in the Plan.⁶

Linked health data aggregation

The individual health data, described in Stream 1: Future focused healthcare - action area, A and B, the Consultation Draft of the Primary Healthcare 10 Year Plan (Consultation), shows that organisations,

The APF – Australia’s leading public interest voice in the privacy arena since 1987

departments and agencies participating in the Plan may store information holdings in separate management systems, indicating data will be aggregated and linked for specific purposes.¹ Recent media attention to real world breaches of aggregated data and Electronic Health Records using APIs highlight APF concerns about the privacy and security mechanisms controlling such data storage.² The APF acknowledges that information security and privacy controls are never absolute. But organisations, government agencies or departments covered by the Plan, where they aggregate sensitive digital health data and link these supported by APIs, must commit to ongoing control of well understood risks as well as regular audits and refreshment of these controls to ensure community confidence.^{3,6-7}

Trust is the foundation of useful community and individual healthcare but seems increasingly overlooked in health authorities' search for cost containment, perceived efficiencies, convenience and access to health research information, a risky approach. The risks might not often play out in public life, but when they do, these risks can prove really damaging to people and to the future of Australian digital health care more generally.

Consent

The APF is heartened by reference to consent in Stream 1, action area B, and Stream 2, person centred primary health care, supported by funding reform.¹ Effective person centred health care revolves around an individual, so seeking 'active consent' from them is paramount here. We ask that the Plan explicitly includes a requirement for 'active consent' rather than simply specify 'consent' in the final version adopted.

Consent for health data holdings nowadays often includes 'pre-ticked boxes' or 'implied consent' rather than 'active consent'. The Plan proposes exponential expansion of present health data collection to biometric and other sensitive health information to be analysed by Artificial Intelligence/Deep Learning algorithms in support of translational medical practice.⁸ The 'active consent' procedure adopted should incorporate clear, freely given, specific, informed and unambiguous indication of the individual's agreement to the collection, holding, management and retention of personal information by all bodies associated with the Plan. Such consent could be obtained by an electronic or oral statement. Silence, pre-ticked boxes or inactivity should not constitute a valid consent.

Privacy legislation

Currently, individuals are not legally protected from the violation of their privacy rights, although this has been 'on the table' since 2008.⁹ The Attorney-General's Department has recently released a discussion paper reviewing the Privacy Act 1988 and a direct right of action for privacy breaches is part of this review.¹⁰ The APF is currently working to analyse the implications of the discussion paper.

Should the Act provide individuals with a direct right of action for privacy breaches in future, it is vital that all tranches of the Plan includes support from a professionally recognised, independent, privacy and security expert that can apply Privacy Enhanced Technologies in the real world. This is not only good practice, but may become a legal requirement if all tranches of the Plan are to prove effective.

Findings from the current MHR GP privacy assessment, conducted by the OAIC, are germane to both operationalising the Plan and to Australian individuals, whose sensitive health information is currently being stored, aggregated and used by the Australian Digital Health Authority in the context of the national MHR system.⁶

Conclusion

The Plan must be refreshed to take heed of the important APF feedback contained in this response to the Consultation. We would be happy to assist the Primary Health Reform Steering Group with the implementation of a revised and workable Plan that fosters growing community trust in digital health implementations.

Contact

Juanita Fernando, Chair APF Health Committee. M: 0408131535 E: juanita.fernando@privacy.org.au

References

1. Consultation Draft of the Primary Healthcare 10 Year Plan, October 2021. <https://consultations.health.gov.au/primary-care-mental-health-division/draft-primary-health-care-10-year-plan/consultation/intro/>
2. McDonald, K. FHIR storm erupts over scary vulnerabilities in third-party apps, blog, Pulse IT, 22 October 2021. <https://www.pulseitmagazine.com.au/blog/6315-fhir-storm-erupts-over-scary-vulnerabilities-in-third-party-apps#:~:text=Written%20by%20Kate%20McDonald%20on,to%20much%20hoped%2Dfor%20levels.>
3. Open Web Application Security Project (OWASP). Top 10 web application security risks. <https://owasp.org/www-project-top-ten/>
4. Australian Digital Health Agency (ADHA). My Health Record, Frequently Asked Questions, 26 November 2018. <https://www.myhealthrecord.gov.au/for-you-your-family/howtos/frequently-asked-questions>
5. Attorney-General's Department. Privacy Act Review – Discussion paper, 2021. Available from <https://www.innovationaus.com/govt-mulls-direct-right-of-action-for-privacy-breaches/>
6. Office of the Australian Information Commissioner. My Health Record access security policy assessment program, 12 August 2021. <https://www.oaic.gov.au/privacy/privacy-assessments/my-health-record-access-security-policy-assessment-program>
7. Open Web Application Security Project (OWASP) OWASP. Top 10 Web Application Security Risks, Available 3 November 2021. <https://owasp.org/www-project-top-ten/>
8. Australian Alliance for Artificial Intelligence for Healthcare (AAAiH). About the Alliance, Available November 1 2021. <https://aihealthalliance.org/about-us/>
9. Australian Law Reform Commission (ALRC) For your information: Australian Privacy Law and Practice (ALRC Report 108) (Report tabled August 2008) <https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/>
10. Privacy Act Review- Discussion Paper. <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/>

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base.

The APF's contributions to policy are based on the expertise of the members of its Board, Committees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, Committees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby AC CMG and The Hon Elizabeth Evatt AC, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies <https://privacy.org.au/publications/by-date/>
- Media <https://privacy.org.au/home/updates/>
- Current Board Members <https://privacy.org.au/about/contacts/>
- Patron and Advisory Panel <https://privacy.org.au/about/contacts/advisorypanel/> The following pages provide outlines of some of the campaigns that the APF has conducted:
- The Australia Card (1985-87) <https://privacy.org.au/About/Formation.html>
- Credit Reporting (1988-90) <https://privacy.org.au/campaigns/consumer-credit-reporting/>
- The Census (2006) <https://privacy.org.au/campaigns/census2006/>
- The Access Card (2006-07) <https://privacy.org.au/campaigns/id-cards/hsac/>
- The Media (2007-) <https://privacy.org.au/campaigns/privacy-media/>
- The MyHR (2012-) <https://privacy.org.au/campaigns/myhr/>
- The Census (2016) <https://privacy.org.au/campaigns/census2016/>