



**Australian
Privacy
Foundation**

<http://www.privacy.org.au>

Secretary@privacy.org.au

<http://www.privacy.org.au/about/contacts>

December 13, 2021

Stephen Issa
Chief Digital Officer
Australian Digital Health Agency
Scarborough House
7/1 Atlantic Street
Woden
ACT 2606
interoperability@digitalhealth.gov.au

Re: Draft National Healthcare Interoperability Plan 2021

This submission by the Australian Privacy Foundation (APF) responds to the Draft National Healthcare Interoperability Plan 2021.¹

The APF, the nation's preeminent civil society body concerned with privacy, voices community concern about the draft Plan based on our focus on the data protection, privacy and information security expectations of patients, their families and communities, clinicians and others affected by sensitive personal information in healthcare data systems. Information about the Foundation appears at the end of this submission.

BASIS

The submission builds on the Foundation's various submissions dating back to the mid-2000s regarding the development and establishment of a national Electronic Health Record,² including long term engagement with NEHTA and the Personally-Controlled Electronic Health Record project which became the My Health Record (MHR).

The submission is made on a non-partisan basis.

SUMMARY

Commendable

- The draft Plan embodies commendable elements, such as open, standards-based, interoperable administration of health information records and, notably, the attempt to support a central role for individual consent and control

Concerns

- The draft Plan signals an expanded use of Individual Health Identifiers, issued to every Australian citizen for their healthcare, while eliminating some of the legislative protections that are currently embodied in the *Healthcare Identifiers Act 2010*³
- The APF is confused by some claimed, unsubstantiated, 'stakeholder benefits' outlined in the draft Plan
- The draft Plan consistently offers false 'security' guarantees pertaining to aggregated, sensitive, individual health information collected, stored, used and disclosed via the MHR system.

Fears

- The draft Plan seems to exacerbate the balkanisation of Australian health privacy protection and is likely to impede national business efforts to achieve an all-important 'Adequacy' decision from the European Commission
- The unspecified and expanded role of IHIs, outlined in the draft Plan is worrying in view of the current, increasingly fragmented and incomplete state of health privacy protection for Australians.

DETAILED SUBMISSION

Commendable

The draft Plan embodies commendable elements, such as open, standards-based, interoperable administration of health information records and, notably, the attempt to support a central role for individual consent and control over who can access one's sensitive, personal information in the medical and health context, including how it should be permitted to be used for the primary purpose of their healthcare.¹

For this element to function in the real world, it is fundamentally important that –

- The Australian Digital Health Agency (ADHA) explicitly takes on board a requirement for 'active consent', a concept which embraces the best, properly informed, most respectful features of real consent, rather than simply specify 'consent', which all too often includes 'implied consent', an invitation to lawyers to find a technical basis for a claim to have informed consent where there is effectively none in reality.
- Given the proposed exponential expansion of data linkage between the federal government's MHR system and State and Territory health data records using the Individual Health Identifier (IHI), outlined in *Section 3.1*, this 'active consent' should be in the form of clear, freely given, specific, informed, un-bundled and unambiguous indication of the individual's agreement to the collection, use, disclosure or retention of personal information by government health authorities and their effective understanding of both the functional steps being proposed and also their implications and potential risks, including long term or rare, but serious, risks.¹ Such active consent could be obtained by an electronic or oral statement. Silence, pre-ticked boxes or inactivity should not constitute valid consent. Nor should acquiescence to unnecessarily bundled 'consent for everything', or where the context does not permit properly informed consent - transparency is 'everything'.
- Active consent from individuals is required and logged every time an MHR data holding is collected, used or disclosed for research and other secondary use purposes. In the age of mature, personalised, big data systems and the failure of promises of impregnable IT system security, it is no longer unrealistic to expect such proper transaction-level logging, accessible to the individual, for data access as part of a privacy-respectful, secure and well governed information architecture, given that it deals with the most sensitive, high risk personal information about almost every individual in the population.

We are glad to note that developing the MHR consent and control framework is a short-term goal listed in the draft Plan and in paragraphs nested inside *Section 6.1. The case for reform.*⁽¹⁾ Controversies, disappointments and failures have plagued the Personally Controlled Electronic Health Record/MHR program and its function in undermining expectations of medical confidentiality between clinician and patient in favour of access by third parties outside the clinical relationship of trust. So it is important that this long neglected aspect of the MHR is indeed now treated as a priority, and addressed in a way that puts patient personal information security and privacy back at its core by means of early, open, wide consultation with patients, advocates, citizens and others outside the 'would-be healthcare data users club'.

Concerns

Community trust is a foundation of the draft, dotted throughout the Plan. But several elements expressed in it seed key APF concerns:

- The Foundation expresses deep concern about short term goals regarding the IHI outlined in the draft Plan. The goals expand the use of IHIs while eliminating some of the legislative protections for individuals that are currently embodied in the *Healthcare Identifiers Act 2010*³, protections, which were integral to its passage into law. Neither the proposed changes nor the consultation framework underpinning these amendments are articulated and remain opaque.¹

Quietly removing essential data protection once a system is running suggests the contemptuous 'bait and switch' tactics used in marketing; this is a common practice in the 'incremental creep' strategy of bureaucratic and corporate attacks on privacy seen all too often in Australia. This potentially unethical approach also undermines the basis for community trust and good-faith support of health data systems that, for instance, have enabled the adoption of exceptional, extremely intrusive practices around Covid pandemic data because the data protection provisions seemed trustworthy.

It is critical to avoid acting in a way that gives any basis for further distrust of central government IT data systems in this area, which are already controversial and not always reliable or effective.⁴

- The APF is confused by some claimed ‘stakeholder benefits’ outlined in the draft Plan. *Section 2.1 Background* describes a consultation process involving a wide range of stakeholders.¹ We wonder which category of stakeholder accrues each of the benefits outlined in *Table 1.1 Horizons for Interoperability actions*, assuming that stakeholders did not provide homogeneous feedback and do not necessarily share the same interests or exposure to potential data-related risks.¹ For example, we query whether patient stakeholders supported the *Reporting to and retrieval from medical device registries at point of care* category in *Section 7.4 Interoperability initiatives*.¹

The lack of important detail, stratifying key points by stakeholder category, in the draft Plan is compounded by ‘benefit’ statements throughout the document.¹ We cannot locate any transparent data supporting the findings reported in the draft Plan. In addition, risks around privacy, personal information, security and data confidentiality, while mentioned in passing, are not recognised in the report in a robust way as a central part of the core problems in trustworthy stewardship of medical and health records (statutorily recognised as the most sensitive form of personal information) in a world where deliberate or unwitting/‘benevolent’ abuses and unwanted uses are on the agenda for many powerful professional, commercial, government and research stakeholders.⁴ In Australia, these stakeholders are uniquely unrestrained by the risk that patients or others whose data may be abused can sue them, as they can in most other peer jurisdictions; so it is critical that discussions about ‘stakeholder benefits’ are most robust, both identifying what interests of which stakeholders are benefited in each case, but also and more importantly, which interests of other stakeholders, especially the vulnerable and weak stakeholders such as patients or their families and communities may be compromised, downgraded or put at risk.⁴ This failure to balance the simplistic and enthusiastic ‘case for reform’ with recognition of the complexities, and sometimes conflicting counter interests or risks for weaker stakeholders, is a core weakness of the document, one which undermines its claims to acceptance.

- The draft Plan consistently offers false ‘security’ guarantees pertaining to aggregated, sensitive individual health information collected, stored, used and disclosed by ADHA. But as the truism goes, information security is never, and can never, be absolute. Aggregated information is a honeypot for miscreants and opportunists, regardless of administrative security controls or good intentions. Health data theft is endemic globally and criminals (and others) find it financially worthwhile to invest in research supporting new ways to steal, analyse, access or ransom health information.

In addition, these aggregated data are also honeypots for other forms of ‘authorised’ access which may be outside the consent of the data subject but difficult for operators to resist, especially when scope creep and incremental expansion are built into the design thinking and the risks and interests of data subjects in Australia cannot be enforced by litigation over negligent data protection or non-consensual use and abuse. Database administrators can merely develop post-hoc, ‘patch up jobs’ to ameliorate new criminal exploits or security vulnerabilities, while hopefully, but not reliably, trying to control known information security and privacy threats. Embedding ‘guarantees’ of security in the draft Plan is quite unrealistic in the current environment, where no one can any longer credibly promise they can keep out all ‘motivated intruders’.

Such unenforceable ‘happy talk’ promises, made safe in the knowledge that in Australia governments have rejected giving individuals the right to pursue breaches in court, simply ensure the loss of community trust in the proposed interoperable system the very first time that a security breach occurs and is available in the public domain, and for well-informed cyber security observers, even before that, since such promises themselves are now neither credible nor enforceable, and thus perform only a marketing function (a deceptive one at that).

The real issue is that large collections of online digitised sensitive personal information are now no longer simply ‘the new oil’, an unalloyed good: they are also potentially unprotectable ‘toxic assets’, since the open-ended price of attempted protection, even if it is paid in full, does not ensure the risks can be avoided. In Australia, the price of failure will be paid by the data subjects, not the stewards (unlike in other jurisdictions where breaches of privacy and data security can and are litigated). Rather than making such implausible and misleading ‘guarantees’, given that data breaches are essentially inevitable and not prone to good intentions, best efforts or a ‘guarantee’ of security, it is important instead to adopt strategies and practices which assume there will eventually be a breach, and thus that ‘data minimisation’ is the more reliable approach.

A discussion of this is beyond the scope of our submission, but it is disappointing to see no recognition or discussion of the issues of the failure of IT security in the face of ever more powerful and sophisticated threats (ones that not even the

most well-resourced national security entities can withstand); the singularly weak position of Australians when their health data privacy is breached; or the emerging centrality of data minimisation approaches to deal with a real world where data breaches will occur and those responsible in Australia at least can be sure to escape responsibility.

Fears

- The draft Plan seems to exacerbate the balkanisation of Australian health privacy protection, and is likely to impede national efforts to achieve an all-important ‘Adequacy’ decision from the European Commission in respect of hosting or dealing with personal information relating to those protected by European laws and standards. The Commission covers Law Enforcement Rules applying to the General Data Protection Regulation framework and the lack of an ‘Adequacy’ decision hinders Australian health businesses, universities and other organisations that deal with customers, research funding and/or service provision in Europe.^{5,6}
- An IHI has been issued to every single Australian, regardless of MHR opt-out. Arguably, it is the most sensitive piece of government data or metadata about individuals we have to uniquely identify patients for healthcare.^{7,8} The unspecified and expanded role of IHIs, outlined in the Plan is therefore worrying, especially in view of the increasingly fragmented and incomplete state of health privacy protection for Australians. In many ways, the new IHI role, combined with prospective, unnamed legislative amendments to the *Act*³, may result in the development of a de facto national identification system framework. It is disappointing that the potential role of an IHI to assist erosion of privacy by this means is not recognised and addressed.

CONCLUSION

Progressing the draft Plan should take heed of the important APF feedback in this submission. We would be happy to assist with the formulation of a workable Plan that fosters a growing community trust in national digital health privacy implementations.

Yours sincerely

Dr. Juanita Fernando,
Chair, Health Committee &
Vice-Chair
Australian Privacy Foundation
juanita.fernando@privacy.org.au

REFERENCES

1. Australian Digital Health Agency (ADHA). Draft National Healthcare Interoperability Plan. Available from https://file-au.clickdimensions.com/digitalhealthgovau-a5xdx/files/draftnationalhealthcareinteroperabilityplan-october2021.pdf?1634876959972&_cldee=anVhbml0YS5mZXJlYW5kb0Btb25hc2guZWR1&recipientid=contact-a5acbe9fe711e811814ce0071b661681-112121acf3d441c7824662cf574c628d&esid=7619d903-7b0c-ec11-b6e6-00224810b2ce
2. Australian Privacy Foundation (APF). APF feedback about the Draft Concept of Operations (ConOps): Relating to the introduction of a Personally Controlled Electronic Health Record (PCEHR) system, 30 May 2011. <https://privacy.org.au/Papers/NEHTA-ConOps-110530.pdf>
3. AustLII Healthcare Identifiers Act 2010. Available http://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/hia2010199/s27.html
4. Alkhatib, S., Kelly, R., & Waycott, J. et al. Who Wants to Know all this Stuff?: Understanding Older Adults Privacy Concerns in Aged Care Monitoring Devices, Interacting with Computers, 24 November 2021. <https://doi.org/10.1093/iwc/iwab029>
5. Johnston, A. Privacy law reform in Australia, - the good, the bad and the ugly, Discussion paper; 3 December 2021. Salinger Privacy. <https://www.salingerprivacy.com.au/2021/12/03/privacy-act-reform-proposals/>
6. Witzleb, N. Data privacy: stricter European rules will have repercussions in Australia as global divisions grow, The Conversation: July 31, 2020. <https://theconversation.com/data-privacy-stricter-european-rules-will-have-repercussions-in-australia-as-global-divisions-grow-142980>
7. Miskelly, G. & Doherty, P. Inside the police database that holds 40 million private records and any police officer can access, ABC News; 23 June 2019 <https://www.abc.net.au/news/2019-06-23/nsw-police-database-privacy-breach-exposed-in-abc-investigation/11224426>
8. Davidson, J. ‘Terrible mistake’ could send execs to jail over vaccine certificates, AFR, . <https://www.afr.com/technology/terrible-mistake-could-send-execs-to-jail-over-vaccine-certificates-20211015-p590am>

Australian Privacy FoundationBackground 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/>