

Statutory Review of the *Data Availability and Transparency Act 2022 (Cth)*

Submission

Population Health Research Network

August 2025



ABOUT THE PHRN

The Population Health Research Network (PHRN) is one of Australia's premier national research infrastructures, advancing innovation through the secure linkage, management and use of high-quality health and human services data. By partnering with researchers, government, industry and the community, PHRN equips Australian researchers with a competitive edge to conduct transformative, data-driven research. Hosted by the University of Western Australia, the PHRN plays a critical role in driving health and social research excellence nationwide. The PHRN is funded by the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

Our Roles

- We are a respected, independent and trusted broker, valued for bringing governments, organisations, individuals and data together securely.
- We collaborate to enhance and maintain significant, innovative research infrastructure to improve the nation's data linkage capability.
- We facilitate and grow the use of linked data in the areas of health and human services.
- We advocate for an improved authorising environment for better access, use and sharing of data.
- We support the whole of government focus on accessing, sharing and using data for the national good.

Our Vision

Linking life data to improve the wellbeing of all Australians

Our Mission

To lead and enable the linking of data for world class, action-oriented research

Contact

Prof Rebecca Glauert
Chief Executive



www.phrn.org.au

Dr Felicity Flack
Senior Manager, Strategy and Services



PHRN RESPONSE TO THE STATUTORY REVIEW – DRAFT FINDINGS AND RECOMMENDATIONS

Overview

The PHRN welcomes the opportunity to further contribute to the Statutory Review of the *Data Availability and Transparency Act 2022* (the DAT Act). The PHRN broadly agrees with many of the draft findings and recommendations made by the Independent Review, including that the DAT Act should be retained but amended to enable more streamlined data sharing practices in a safe and consistent way.

The PHRN particularly welcomes the Review's finding that the complex and highly prescriptive processes embedded in the DAT Act operate as a barrier to the effective uptake of the Scheme. Such processes do not equate to greater protection of information; instead, they create confusion and increase the regulatory burden on entities seeking to collect, use and disclose information. Long-term, this complexity is likely to propagate an inimical culture of reluctant data-sharing and restricted data-use. The PHRN agrees that the DAT Act should be 'stripped back to its essential elements with significant parts reformed or removed'.¹

The protection of information disclosed under the Act remains important. Protective mechanisms play a central role in facilitating and maintaining public trust in, and the social licence of, data sharing² and are particularly relevant in the context of the DAT Act's secrecy override provisions. In the PHRN's view, such protections are best implemented through confidentiality requirements and conditions associated with accreditation, rather than through prescriptive requirements that apply regardless of the level of risk involved. Further, data should only exit the Scheme in very limited circumstances, where data has been de-identified and aggregated.

The Review also focused on the role of the Office of the National Data Commissioner (ONDC) and made several suggestions regarding the ONDC's functions and powers. In the PHRN's view, it is important that the ONDC is retained, and that the National Data Commissioner (NDC) continues to serve a compliance, monitoring and enforcement role. Presumably, as the Scheme matures and uptake increases, the need for the ONDC to perform these functions will intensify. An independent body with specialist expertise in data sharing is best placed to adjudicate disputes and complaints arising from the Scheme. The ONDC's educative functions should also be retained. With the simplification of the DAT Act, and in conjunction with other proposed amendments, the guidance, education and support offered by the ONDC is likely to be of increased value in encouraging and facilitating data-sharing in future.

The PHRN also supports the introduction of timeframes for decision making, a requirement for the provision of detailed reasons for refusals, and a robust appeals process. As the Review has identified, increased investment and resourcing will be necessary to enable agencies to meet these requirements.

¹ Australian Government Department of Finance, *Statutory Review of the Data Availability and Transparency Act 2022 – Draft Findings and Recommendations* (July 2025) 9.

² See generally: Judy Allen, Carolyn Adam and Felicity Flack, 'The Role of Data Custodians in Establishing and Maintaining Social Licence for Health Research' (2019) 33(4) *Bioethics* 502; Pam Carter, Graeme T Laurie and Mary Dixon-Woods, 'The Social Licence for Research: Why Care.Data ran into Trouble' (2015) 41 *Journal of Medical Ethics* 404.

The DAT Act must be amended to reduce its complexity, increase its flexibility and ensure that it remains relevant and adaptive to future technological changes and challenges. The DAT Act should provide a simple, clear authorising pathway for the collection, use and disclosure of information, whilst maintaining public confidence in the confidentiality and privacy protections it offers. Rather than functioning as an alternative pathway, the DAT Act should be looked to as **the** enabling mechanism for Commonwealth data sharing activities in Australia and should be the model to which other Australian jurisdictions look when seeking to develop mirror legislation that in turn, facilitates a nationally consistent, fully interoperable data sharing framework.

Response to the Draft Recommendations

Recommendation 1: The DAT Act should provide a clear authorising pathway that enables sharing of Commonwealth data for approved purposes.

The PHRN supports this recommendation.

The DAT Act should function as a clear authorising pathway for the sharing of Commonwealth data. Whilst it should be technically capable of operating alongside other data sharing pathways, the PHRN suggests that it should act as the primary data sharing pathway, rather than merely an alternative as the Review suggests. The sharing of data under other legislation is often permitted as an exception to a confidentiality requirement, or where it is certified to be in the public interest with little guidance on parameters or reasons given for how such an assessment is made. With significant amendments, the DAT Act has the capacity to become a safe, consistent, best practice pathway through which data is reliably shared. The cost of implementing the Review's recommendations, together with the investment required to upscale concomitant resourcing, is less justifiable if the DAT Act is simply intended to function as one option out of many; rather, it should be the first port of call for entities seeking access to Commonwealth data for approved purposes.

Recommendation 2: The DAT Act's data sharing authorisation framework should be simplified, and its requirements streamlined to reduce complexity and support ease of use.

The PHRN supports this recommendation.

The PHRN agrees that the DAT Act 'should move away from its highly prescriptive, granular conception of data sharing projects, participants and roles to facilitate greater flexibility'.³ A principles-based approach has the capacity to provide this flexibility and, to an extent, 'future proof' the Act with respect to future technological changes and challenges. However, and as the ALRC has identified, principles-based, outcomes-focused systems also have the potential to create uncertainty and inconsistencies that affect the robustness of the protections provided.⁴

The PHRN supports the adoption of a 'hybrid' approach, in which broad, high-level principles are 'supplemented by more specific rules in regulations or other legislative instruments'.⁵ For example, a high-level requirement for entities to make reasonable efforts to protect data from misuse or loss could be supplemented by more prescriptive conditions set out in regulations regarding systems and security procedures. Clear statutory criteria for the disclosure of information (for example, it is in the

³ Australian Government Department of Finance, *Statutory Review of the Data Availability and Transparency Act 2022 – Draft Findings and Recommendations* (July 2025) 16.

⁴ Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) 242.

⁵ Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) 242.

public interest, HREC approval has been provided where applicable) should however, be retained in primary legislation. An appropriate body (such as the ONDC) should provide guidance on how the principles should be interpreted and applied, similar to the APP Guidelines drafted by the Office of the Australian Information Commissioner. Some upskilling and investment in the legal expertise of the ONDC may be required.

With respect to data sharing agreements (DSAs) the PHRN submits that DSAs should remain compulsory under the DAT Act, but that the mandatory requirements under s 19 should be removed so that parties are free to negotiate their contents. DSAs are a familiar and useful tool for setting out the parameters of data-sharing, and consistency in the mechanism used for data-sharing under the Act is desirable. However, the DAT Act should be amended to enable DSAs to be scaled back and adapted to increase efficiency and responsiveness to different instances of data sharing, including for different approved purposes. This would still enable a shift away from project-based approvals to sharing for approved purposes in a regulated way.

The PHRN agrees that there is an ongoing need to document data sharing activities and considers that certain information should continue to be made publicly available, although this does not necessarily have to occur via the publication of DSAs (for example, entities could complete an approved form that is then published on the ONDC website). Public access to such information is important for maintaining trust, promoting transparency, and providing individuals and entities with the information to decide whether there is a potential basis for making a complaint. The PHRN submits that, at minimum, the following key information should be made publicly accessible:

- The reason for the sharing i.e., the approved data/sharing purposes
- The identity of the entity receiving the data
- How data will be stored
- How long the data will be retained; and
- Whether the shared data contains identifiable information.

Recommendation 3: The DAT Act's settings should be more flexible and proportionate, clearer and more easily adaptable to different data sharing activities.

In the PHRN's view, aspects of this recommendation are somewhat unclear. For example, it is not apparent which 'settings' are encapsulated in this recommendation, or what specifically is meant by authorised 'use-cases'.⁶As stated above, the PHRN's view is that increased flexibility in the Act is desirable and that this can be largely achieved through implementing a hybrid principles-based approach. Additionally, broadening the 'approved purposes' under the Act, which would enable the creation of enduring linked assets (see our response to Recommendation 12 below) would increase the uses to which data may be put without compromising necessary protections.

However, and in the absence of further information as to what these reforms might look like, the PHRN does not support the proposal to 'recalibrate' privacy safeguards, or the proposal to increase the operability of the DAT Act with other data sharing frameworks so that data can more readily exit the Scheme. It is not clear that the protection offered by other frameworks will be sufficient to account for the sensitivities of certain types of data that may be shared under the DAT Act (using the override provision in s 23) that would otherwise be subject to greater restriction. Excluding privacy legislation,⁷

⁶ I.e., should this be understood by reference to approved purposes or is it better equated with data sharing activities or projects?

⁷ Better characterised as 'data protection', rather than 'data sharing' legislation.

it is also not apparent how these frameworks would operate to regulate such information where it has already been disclosed.

In light of the Review's recommendations to expand both the entities eligible for accreditation and the approved data sharing purposes under the Act, it is particularly important to ensure information does remain protected, regulated, and under the enforcement regime and oversight of the ONDC.⁸ This does not prevent the Review's objective of data assets and insights being 'more readily re-used and deployed or released';⁹ however, such sharing should occur within the scheme between accredited entities for approved purposes. The 'release' of data, for example to include statistics in publicly accessible annual reports or findings in published research articles, could occur on a limited basis, and only where data has been aggregated and/or de-identified.

Recommendation 4: The DAT Act should support a default posture of agreeing to share data, with data custodians able to refuse requests in appropriate circumstances.

The PHRN supports the introduction of statutory reforms that facilitate and encourage the increased sharing of public sector data. However, the PHRN is concerned that incorporating a positive obligation to share data into legislation may have unintended consequences. Such a requirement is something of a blunt instrument and has the potential to undermine public trust in the government's ability to protect sensitive information. It may also, inadvertently, create a culture where data-custodians concerned about risk and their legal liability for sharing data shift their focus to finding justifications for refusal. In the PHRN's view, other measures (such as the introduction of reasons for refusal, and an audit of data custodian decisions, see below) are likely to be more effective at ensuring that requests are only rejected with good reason.

Submissions as to whether a mechanism for identifying a 'primary' data custodian, or whether a unilateral discretion over data sharing decisions should be introduced are best left to data custodians. State and territory data custodians are legally obliged under their own legislation to protect and manage data, and their data-sharing agreements with the Commonwealth typically allow them to control who can access it to manage their liability. Removing this control could lead custodians to stop supplying data to the Commonwealth, as they are under no obligation to do so and the DAT Act cannot compel them. However, the PHRN does believe that it is important to streamline decision making as much as possible, and to ensure decisions are consistent. Investment in data custodians' training and education, and the implementation of clear criteria and guidelines on decision-making are necessary for this to occur. Any training and resources should be developed, conducted and distributed by the ONDC (following initial consultations with data custodians for maximum uptake) to ensure a consistent approach.

Similarly, the PHRN agrees that clear requirements and parameters for data sharing decisions should be introduced. We suggest this is best implemented through subordinate legislation, to keep pace with changing technology and security requirements. Enshrining the decision-making criteria in subordinate legislation will help to ensure that they are transparent and will support consistent decision making. Additionally, reasons for a refusal to share data should always be provided. The PHRN suggests that such reasons be made publicly available, as a matter of transparency and so that other data requesters can see precedents for what has not been approved. Alternatively, the ONDC might be tasked with conducting a regular audit of such decisions to ensure they are rationale, reasonable

⁸ Note this does not preclude the ONDC referring matters to the Australian Information Commissioner under s 107 of the DAT Act. This feature should be retained.

⁹ Australian Government Department of Finance, *Statutory Review of the Data Availability and Transparency Act 2022 – Draft Findings and Recommendations* (July 2025) 17.

and consistent, although this will not provide the same level of transparency, in the absence of publicly available reasons for decision.

The PHRN also supports the introduction of timeframes for decision-making. Whilst suitable timeframes should be decided through consultation with data custodians, we suggest that a range (rather than a fixed number of days) may be appropriate to enable flexibility during staffing shortages and periods of increased demand. This will necessitate increased investment and resourcing.

The PHRN also strongly agrees with the implementation of an appeals process. In the PHRN's view, these appeals should, in the first instance, be made to a higher entity/established body within the relevant data custodian's public sector agency with the appropriate expertise to understand the data custodian's practices, constraints, and the data involved.¹⁰ Timeframes for the appeals process and a requirement to publish reasons for the appeal decision should be implemented. The PHRN suggests that, in the event of a dispute, the matter is initially referred to an independent mediator certified by the ONDC as having the necessary expertise to assist with these matters. If the issues cannot be resolved at mediation, and the data custodian ultimately refuses the request, data requestors should have the option to appeal. If data requestors are dissatisfied with the result of the appeal, there should then be a mechanism for appeal to an external entity.

Recommendation 6: The National Data Commissioner's functions and powers should be reformed to focus on assurance, oversight and assistance in facilitating data sharing decisions.

In the PHRN's view, monitoring and compliance remain very important. The need for the ONDC to fulfil this role will likely increase as the scheme moves into maturity and becomes more heavily utilised. As noted above, it is not sufficient to rely solely on privacy legislation for enforcement and compliance; different issues may arise in the context of sharing under the DAT Act, and the secrecy 'override' provision necessitates clear and continuing regulatory oversight by a designated, appropriately empowered statutory authority.

We also note the potential problems that may arise if the ONDC retains its enforcement and compliance capabilities but is also provided with the power to inquire into, review and make specific recommendations about data sharing projects. Issues may arise if, for example, there is a dispute about a provision or requirement that was implemented at the recommendation of the ONDC. In our view, the guidance provided by the ONDC should be similar to that provided by the OAIC in respect of privacy issues, and the ONDC should fulfil a similar role in terms of breaches of the DAT Act and Scheme complaints. As suggested above, independent mediators certified by the ONDC could play a role in mediating negotiations between data requestors and data custodians. Mediator certification may require evidence of familiarity with data sharing and/or mandatory mediation and data-sharing training activities hosted by the ONDC. As part of this, and as a consequence of other recommendations, the PHRN supports expanding resources of ONDC.

Recommendation 7: The DAT Act should establish a permissions-basis for accreditation which replaces the current strict 'user' and 'data service provider' accreditation designations

The PHRN supports Recommendation 7.

¹⁰ Note that this is different to the ONDCs review of complaints regarding breaches of the Act or DSAs under the Act, which should be retained.

A permissions-basis for accreditation that does away with designated, project-specific roles and enables accredited entities to perform actions subject to the conditions of their accreditation is sensible and will assist to streamline data sharing.

The PHRN supports a continued mechanism for review and appeal of conditions imposed as part of the accreditation process, and for the removal of conditions upon evidence of upskilled capabilities. Entities should remain under an obligation to report any changes that may affect their accreditation status.

Recommendation 8: Explicit accreditation ‘tiers’ should be introduced to more simply reflect different accreditation standards and to facilitate alignment between accreditation and data sharing use-cases.

The PHRN does not, however, support Recommendation 8 and the introduction of accreditation ‘tiers’. Introducing tiers is likely to add back a level of complexity into the process and does not appear necessary under a permissions-basis approach, where conditions are tailored and imposed on a case by case basis following assessment, on the basis of evidence, of an entity’s capabilities and constraints. Further, whilst a higher ‘tier’ accreditation status might ostensibly act as greater encouragement for data custodians to share data, it may also have the converse effect and ‘screen out’ lower tier entities without fair consideration of their capacity relative to the proposed data use.

Recommendation 9: Transparency and other measures which promote greater regulatory flexibility should be introduced and have consideration to broader developments in the data system.

The PHRN generally supports the inclusion of transparency measures within the Act that promote clarity and consistency in accreditation decisions. Specifically, the PHRN supports the retention of current provisions that require reasons to be provided for any refusal of accreditation and for any conditions imposed.¹¹

As outlined in our first submission to the inquiry, rules that prescribe evidentiary requirements should be designed simply and flexibly so as to allow entities to provide a range of evidence and assurances as part of demonstrating their ability to meet requirements. Similarly, the PHRN also suggests that data custodians work closely with the ONDC to eliminate duplicative approval and accreditation processes. For example, information that is relevant to the approvals process, that has already been provided to the ONDC as part of the accreditation process, could be (with entity approval) directly accessed by the data custodian without the entity needing to re-supply it. Further consultation with the ONDC and data custodians about how this can occur would need to take place.

Recommendation 10: The entities that can seek accreditation to request and use data under the DAT Act should be expanded to include ACCOs, not-for-profit research institutes (including independent research organisations and medical research institutes), primary health networks, and not-for-profit service delivery organisations (including approved aged care providers).

The PHRN supports this recommendation.

Additionally, and after further consideration, the PHRN suggests that the DAT Act be ‘opened up’ to any entity, including the private sector, that is able to meet the accreditation criteria.

¹¹ *Data Availability and Transparency Act 2022* (Cth) s 75(2)(d)(ii), s 75(3)(a).

Considerations specific to the private sector, for example the use of data for commercial purposes, are better regulated through specific provisions in the primary legislation that restrict (if desirable) such uses, rather than the wholesale exclusion of ‘private’ organisations, many of which serve an important public function, are not-for-profit and/or receive government funding. Expanding the categories of entities that are eligible to participate in the Scheme in a piecemeal fashion has the potential to create unnecessary, definitional complexities that may inadvertently exclude the same or similar types of entities from being able to access data under the Act as a result of specific governance, incorporation, or funding arrangements.

As a related matter, opening up the DAT Act to enable wider accreditation is a further reason to make it more difficult for data to exit the scheme.

Additionally, in our view and with respect to Recommendation 11, a broader initial starting point for eligibility is preferable to a Ministerial power that enables the Minister to expand accreditation eligibility in specific cases. It is not clear when exactly it would be appropriate for this to occur, or what the relative weight accorded by the ONDC to different considerations would be when providing its advice, which creates the potential for inconsistency and lack of transparency in decision-making. Such an approach has the potential to undermine the integrity of the Scheme and the protections it offers.

Recommendation 12: Expand the data sharing purposes to include data curation and the creation of data assets.

The PHRN supports this recommendation.

Specifically, the PHRN submits that s 15 of the DAT Act should be amended to include the following data sharing purposes:

1. The creation of research infrastructure, enduring data linkages and data assets
2. Data curation
3. The management, funding, evaluation, or monitoring of services, including quality improvement and assurance activities
4. The compilation or analysis of statistics.

The current approved purposes of delivery of government services; informing government policy and programs; and research and development should be retained.

Expanding the approved purposes to permit data sharing for a broader array of public health and wellbeing purposes will increase the relevance, effectiveness and uptake of the Act. Specifically providing for the creation of enduring data assets and including data curation as separate, approved data-sharing purpose will remove many of the complexities that presently arise when these activities are undertaken as part of, or to facilitate the achievement of, various approved projects. Any sharing of information from the data asset created under the DAT Act should remain under and be subject to the DAT Act; for example, it would need to be for an approved purpose and presumably with the consent of the entity that created the asset, and the entities that supplied the data (ie, multiple data custodians).¹² The Act or associated regulations should also make it clear that both data linkage, and the disclosure of information to enable data linkage to occur to facilitate sharing for an approved purpose, are permitted.

As part of shifting away from a specific project approval model, and to enable the better ‘re-use’ of data by accredited entities, the DAT Act should also explicitly permit sharing for more than one

¹² Although approval could be ceded with conditions to one entity under the relevant data sharing agreement.

approved purpose.¹³ Entities are often hindered by concerns over the appropriate secondary use of data and would benefit from clear, unambiguous authorisation to collect and use data for multiple approved purposes under the Scheme. Such authorisation would likely reduce organisational cost and resource requirements and increase the efficiency and effectiveness of the activities undertaken. Provided the sharing and use occurs in accordance with the DAT Act, DAT Regulations, the DSA, ONDC guidance, and any other applicable requirements (such as HREC approval for research) it is difficult to see how single sharing for multiple purposes will pose additional risk to the security or integrity of data.

Recommendation 16: Longer term, there should be a nationally consistent data sharing framework that achieves full interoperability across jurisdictions and provides standardised pathways for users to access any Australian public sector data; **Recommendation 17:** Continued investment in the broader data sharing ecosystem is required to cultivate improved and sustained data sharing outcomes.

The PHRN supports these recommendations.

With respect to the example provided under Recommendation 16, we do, however, note that data that exits the framework should not include identifiable data (such as household address information or the names of home residents), and should only occur in limited circumstances. The example provided involves state governments using an integrated data asset created under the Scheme for a broad range of purposes, including to update its customer record information and notify individuals of their eligibility to receive a particular grant. It is not clear from this example why the household address information and names of home residents would need to exit the Scheme for this to occur, or why this would not fall under an approved purpose of delivering government services and/or informing government policy and programs. Where other eligible entities are interested in such data, applications should be made to access the data directly from the national integrated data asset (rather than through state and territory governments), which also prevents the need for data to exit the scheme and centralises decision-making.

With respect to Recommendation 17, the PHRN supports a general uplift of the data sharing ecosystem, and increased investment in the infrastructure, technical proficiency, education, and resourcing of data custodians. Investment and funding should be considered and distributed carefully, and inter-agency cooperation encouraged, to maximise investment benefits and create a culture of collaboration rather than competition between agencies. Whilst submissions as to the most appropriate agencies to lead a whole-of-Commonwealth system technical uplift are best left to those agencies, the PHRN notes that both the ABS and the AIHW have significant expertise and experience in this area.

Further recommendations

The substance of the recommendations made above predominantly focus on the ways in which data-sharing may be simplified and streamlined. Given the sensitivity of the information likely to be shared under the Act, and the broad purposes to which it may be put, the PHRN also suggests the Review consider whether strong protective provisions that impose mandatory confidentiality requirements on recipients of data should form part of the amended Act. Such provisions might impose civil or criminal penalties on any collection, use, or disclosure of information that occurs in contravention of the Act and is not otherwise authorised by any other Act or law. We suggest such protections are

¹³ This may also require amendments to the privacy act protections that apply under the DAT Act.

appropriate in light of the Act’s secrecy override provision, and particularly if the Review determines it is appropriate to ‘re-calibrate’ privacy protections as outlined in Recommendation 3.¹⁴ Further, where sharing is authorised under the Act, it should be explicitly stated that such sharing is not in breach of any common law or equitable duty of confidentiality, and that data custodians and recipients are protected from liability in this respect. A provision of this kind is likely to increase the confidence of data custodians and data recipients alike and assist with creating a pro data sharing culture in a safe and regulated way.

Conclusion

The PHRN thanks the Review for the invaluable opportunity to contribute to the Statutory Review of the DAT Act. Should you wish to discuss our submission please do not hesitate to contact us.

¹⁴ Australian Government Department of Finance, *Statutory Review of the Data Availability and Transparency Act 2022 – Draft Findings and Recommendations* (July 2025) 17.