6 November 2020

Department of the Prime Minister and Cabinet
Office of the National Data Commissioner
PO Box 6500
Canberra ACT 2600

To the Office of the National Data Commissioner,

Submission into the Data Availability and Transparency Bill 2020 Exposure Draft Consultation Paper

Thank you for the opportunity to provide feedback on the Data Availability and Transparency Bill 2020 Exposure Draft Consultation Paper. We are:

Positive Life NSW (Positive Life) is the lead peer-based agency in NSW representing people living with and affected by HIV in NSW. We provide leadership and advocacy in advancing the human rights and quality of life of all people living with HIV (PLHIV), and to change systems and practices that discriminate against PLHIV, our friends, family, and carers in NSW.

The HIV/AIDS Legal Centre (HALC) is the only not-for-profit, specialist community legal centre in Australia. We provide free and comprehensive legal assistance to people in NSW with HIV or Hepatitis-related legal matters and undertake Community Legal Education and Law Reform activity in areas relating to HIV and Hepatitis.

Background
The Office of the National Data Commissioner released in September 2020 a draft legislative package for the new Data Availability and Transparency Bill (previously titled the Data Sharing and Release Legislation). Positive Life NSW and the National Association for People with HIV/AIDS (NAPWHA) contributed a submission to the 2018 New Australian Government Data Sharing and Release Legislation Issues Paper for Consultation, and we commend the government for continuing to engage and consult with community and other stakeholders to shape this legislation and the operationalisation of it in the best interests of the Australia public.

Aims
The Data Availability and Transparency Bill (DAT Bill) aims to "modernise the approach to sharing public sector data" and:

- "promote better availability of public sector data
- enable consistent safeguards for sharing public sector data
- enhance integrity and transparency in sharing public sector data
- build confidence in the use of public sector data, and
- establish institutional arrangements for sharing public sector data."[1]

Any discussion of the release and sharing of public sector data must be underpinned by the principle aim of benefit to the Australian public, not commercial or other private gain. The

[1] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Data Availability and Transparency Bill 2020 Exposure Draft Consultation Paper*

aims listed thus far do not specifically propose to benefit the Australian public. The proposed aims of the DAT bill only address the benefits to external parties of having aggregated data sets made available to them and fails to address the benefits (or potential risks) for individuals or communities. We recommend that the aims be amended to include:

- enhance and support the right to individual privacy of data within the context of the Australian data sharing landscape, and
- improve government services and policies through the sharing of public sector data.

Definition of 'public sector data':
Section 10 - Data Definitions of the DAT Bill Exposure Draft states:
(2) *Public Sector data* is data lawfully collected, created, or held by or on behalf of a Commonwealth body, and includes ADSP-enhanced data.

This definition establishes the scope of government data that can be shared under the data sharing scheme. The term includes data that is collected, created, or held by a Commonwealth body, or on its behalf. Public sector data includes 'personal information' and 'sensitive information', as defined by the *Privacy Act,* as well as other types of data.

We agree that some public data has the capability to strategically benefit the Australian public, contribute to economic prosperity, and improve a range of policy outcomes. We advocate for and support legislation to create more streamlined and efficient processes for sharing and releasing non-personal/sensitive public data held by government agencies. This will contribute to greater transparency, accountability, service efficiency and value, and public trust in government and wider business processes.

We do not support access to and sharing of individual data (including 'personal information' and 'sensitive information'), identifiable or de-identified, for purposes other than that which data was originally collected and having received specific informed consent from the individual on a case by case basis. This is particularly the case given the limitations to existing privacy legislation within Australia and the current state of respect for the fundamental right to privacy and control of personal information for Australian individuals (data sovereignty). Higher-risk datasets which includes those containing 'personal information' and 'sensitive information', by definition, pose an unacceptably high risk to individual Australian's right to privacy and control over their own personal information and data. Data linkage and use of de-identified data needs to be ethically and transparently managed. These processes and policies differ extensively between organisations and government departments, many of which may not be used to handling particular data sets (i.e. sensitive information, including health information) and the 'extra' protections that must be in place therein. There is ample evidence of the simple process of patient re-identification risk in public health records, along with multiple and wide-spread privacy breaches of personal information by inadvertent government organisations, the most recent and high-profile of which is the Department of Foreign Affairs and Trade mistakenly releasing 2,727 individual's email addresses on 30 September 2020,[2] confirming the high-risk nature of data sharing and release, even in secure systems and when data is de-identified.

Data sharing purposes:

[2] Margaret Simons, 'DFAT admits email addresses of almost 3,000 Australians stranded overseas released in breach', The Guardian Australia, 2020, accessible at: https://www.theguardian.com/australia-news/2020/sep/30/data-breach-dfat-reveals-email-addresses-of-vulnerable-australians-stranded-overseas

The DAT Bill aims to limit data sharing to three purposes, which are all intended to ensure data sharing is in the public interest. Section 15 - Data Sharing Purposes of the DAT Bill specifies that data is to be shared for:

- Delivery of government services
- Informing government policy and programs, and
- Research and development.

The Explanatory Memorandum states that the delivery of government services as identified in section 15(1)(a) includes 'activities that provide coordinated and structured advice, support, and service to those engaging with the government.' We agree that efficient delivery of government services may justify the sharing of data by government agencies, but important parameters need to be in place. Although the Explanatory Memorandum states that assurance and compliance activities, such as determining a person's eligibility for welfare payment, would not be a permitted purpose, this does not provide sufficient guidelines for the interpretation of 'delivery of government services'. We strongly agree with the Information Integrity Solutions Pty Ltd.'s (IIS) recommendation to "ensure that the DAT Bill is drafted in such a way that there is no doubt that 'precluded purposes' include compliance and assurance. Amend the Explanatory Memorandum and supporting guidance material to make it clear that compliance and assurance activities are precluded". The DAT Bill should clearly include compliance and assurance as a precluded purpose under Section 15(2). Furthermore, the Explanatory Memorandum should provide clear guidelines as to the definition of 'compliance and assurance activities' including more examples than the one currently provided.[3]

We believe that to achieve the purpose of efficient delivery of services, that government-based (not individual's) public data should be made widely, publicly available for greater transparency and accountability, to facilitate swifter adjustments to services as necessitated by the data made available.

Under subclause (1)(b) of the DAT Bill, sharing to inform design and implement government policy programs is considered a permitted purpose for the sharing of data. The Explanatory Memorandum states that both the terms 'government policy' and 'government programs' should be interpreted broadly and will not directly target individuals.[4] Purposes (1)(a) and (1)(b) must not be overlooked or undermined if and when data accessed by government entities or other accredited users provides proof of a service requirement or adjustment that may be disagreeable to the government entity, particularly when the data is calling for a service or adjustment that would be of significant benefit to Australian citizens but fiscally problematic to the government.

The final permitted purpose under subclause (1)(c) allows data sharing for research and development purposes. Under this purpose, concerns of commercial benefit have been raised and addressed to a certain extent under the DAT Bill.[5] We acknowledge that the Privacy Impact Assessment considered commercial applications for data sharing, and came to the following view: "that possible commercial applications of the data were adequately

[3] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Data Availability and Transparency Bill 2020 Exposure Draft*

[4] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Data Availability and Transparency Bill 2020 Explanatory Memorandum*

[5] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Data Availability and Transparency Bill 2020 Exposure Draft*

checked by the range of protections in place – particularly public interest and ethics requirements but also the Data Sharing Principles more generally, purpose limitation, data minimisation and the requirements contained in Data Sharing Agreements. These create a high bar for sharing to support commercial activities."[6]

We believe that regardless of whether a proposed data sharing project meets one of the three purposes and meets the 'public interest' test, there should be no profit made from the use of the public data shared, and particularly not that of individuals' data. If the request for release and use of public sector data is truly in the public interest, the accredited organisation in question should conduct the project without the additional aim or outcome of making a profit from Australian's data. We recommend that an additional clause on commercial activities require that if any profit is made from the sharing of public data, that a certain proportion of the profit should be donated to the community with which the data sharing is intending to benefit in the 'public interest' test, and which should be acknowledged and agreed upon in the data sharing agreement. This will ensure that the private sector does not take advantage of the data sharing legislation for the purposes of profit-making, whilst only tangentially conducting a project in the 'public interest'.

We acknowledge that there are numerous restrictions in place to preclude certain purposes from the data sharing legislation, such as the sharing of data for national security purposes, for enforcement-related purposes, such as law enforcement, policing, compliance, and assurance activities. We acknowledge that "The Minister may prescribe additional precluded purposes in rules to address future risks. The Minister could only narrow the existing scope and is unable to authorise new purposes for sharing."[7] However, we believe that the permitted purposes scope is currently too broad and should be restricted further, such as through a profit-limitation clause as mentioned above, through the exclusion of 'personal information' and 'sensitive information' from the shareable data sets, and through the explicit exclusion in the DAT Bill of compliance and assurance activities.

Under section 17(4) of the Bill, a provision of law prescribed by the regulations would prohibit a data custodian from disclosing the data in the circumstances in which the sharing is done, or the data custodian of the data as prescribed by the regulations would not be permitted to share data in their capacity as a data custodian. The legislation covered by section 17(4) is to be prescribed by the regulations which would currently exclude data from MyHealth Records and the COVID-safe app being shared. We believe that this measure cannot be sufficiently safeguarded within regulations that may be amended by the Governor-General and should be included in the DAT Bill and subject only to amendments through parliament.

We strongly agree with the IIS recommendation that the DAT Bill: "Address the expected data sharing purposes in the Explanatory Memorandum, giving examples of what would and would not fit within these terms, in particular in relation to compliance. Make clear that private sector organisations could become accredited entities and that any commercial activities must be consistent with the permitted purposes." The rationale for this recommendation was that: "In addition to the proposed principles and controls in the Data Sharing Scheme, there is value in restricting the definition and interpretation of permitted

[6] Information Integrity Solutions, *Privacy Impact Assessment – Draft Data Availability and Transparency Bill 2020*

[7] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Data Availability and Transparency Bill 2020 Exposure Draft Consultation Paper*

purpose under the draft DATB, so as to arrest function creep and expansive uses that go beyond community expectations." The Department stated in the Consultation Paper that they agree with the recommendation and have included descriptions of permitted purposes in the draft Explanatory Memorandum.[8] These descriptions are brief and inadequate, and should be robustly expanded to avoid any future doubt about what constitutes an appropriate permitted purpose for data sharing. Without this guidance, it is difficult to effectively comment on issues that may arise from the proposed legislation and relies heavily on oversight and consideration during future legislative reviews of the Bill.

We also note that the draft DAT Bill excludes data sharing that "would infringe intellectual property rights or international agreements, or where intelligence agencies or their data are involved."[9] We question the DAT Bill's ethical grounding when it intends to protect via exclusion from datasets the intellectual property of private companies but will not exclude from data sets the sharing of individual Australian's own 'personal information' and 'sensitive information'. This is a clear prioritisation of commercial interests over individual rights to data sovereignty, which we believe should be rectified in the DAT Bill by prohibiting the release and sharing of individual information.

Data Sharing Principles:
The DAT Bill intends to provide layers of safeguards, including data sharing principles, to manage risks associated with sharing data. The data sharing principles[10] are intended to be a risk management framework that must be applied to each data sharing project.

"Project Principle: considers the intended use of the shared data, including public interest, consent and ethics requirements."

- This principle needs to be strengthened to include a 'zero-profit' component of public interest and ethical sharing and use of public data, as well as detail about how it will be monitored and guaranteed. Gaining consent from individuals by government departments is a basic requirement that needs to be significantly expanded on in this principle and will be discussed further below.

"People Principle: considers users accessing the data to ensure they can be trusted and have the right skills for the project."

- In outlining the ABS Five Safes Framework in the Consultation Paper, it is clear that although the Data Sharing Principles are modelled off the ABS Five Safes elements, they are significantly lacking in detail and thoroughness. For example, named individuals on projects must be required to undertake training, similar to the mandatory ABS DataLab safe researcher on-boarding before they are provided data access. Additionally, all users must sign comprehensive confidentiality agreements and data usage agreements before granted access, and there must be legal sanctions and penalties written into the DAT Bill if these agreements are breached.

"Setting Principle: assesses if data is shared in a safe environment."

[8] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Data Availability and Transparency Bill 2020 Exposure Draft Consultation Paper*
[9] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Data Availability and Transparency Bill 2020 Exposure Draft Consultation Paper*
[10] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Data Availability and Transparency Bill 2020 Exposure Draft*

- Similarly, this Principle is lacking in detail and thoroughness. It must include specific controls that will be implemented for user access to shared data, similar to that which the ABS Five Safes Framework outlines, such as (but not limited to) two-factor authentication, logging, and auditing of activity, 'need to know' access protocols, and protocols in place to minimise the likelihood of unauthorised use, access, or loss of data. Furthermore, accredited data users must only be Australian, in terms of both individual data users, organisational data users, and the location with which the data is accessed and utilised.

"Data Principle: assists in navigating what data is appropriate for sharing. Only the amount and detail of data that is reasonably necessary to achieve the project should be shared."

- We reiterate our recommendation that 'personal information' and 'sensitive information' are not included in the permitted data sharing sets, as even de-identified data is notably easy to re-identify. No release or sharing of individual Australian data, particularly health data, outside of the original purpose and intent of collecting such data, can be consistently and appropriately safeguarded within the landscape of Australia's current privacy laws. This is particularly the case given a significant amount of data collected about Australian individuals (both citizens and people residing in Australia) is not reasonably required or relevant to the purpose for which that data is collected, and consent for the gathering of this information is regularly uninformed, misinformed, bundled, and/or coerced. If the Department insists on creating legislation that will share individuals' personal data, then this Data Principle must be substantially strengthened to protect the privacy and confidentiality of individuals' data. Part of this strengthening must involve training for accredited users in the responsible use of data including not attempting to re-identify individuals or organisation, and substantial penalties for individual or organisational accredited users who circumvent or do not abide by this.

"Outputs Principle: ensures the results and outcomes of the projects are agreed, including whether they are appropriate for publishing."

- This Principle is also insufficient and must include more detail, monitoring, and assurances, such as vetting and approval by a nominated, impartial data release officer prior to any data release to ensure outputs are consistent with stated aims, purposes, and expected outcomes as well as ensuring re-identification is not possible.

Rights and Responsibilities:

Privacy of all individuals' personal information and data is not only an expectation but a fundamental human right. Privacy is not a privilege or a burden to the government or economic system, nor a constriction to the efficient functioning of governmental processes and policy outcomes. We recommend that the DAT Bill be focused on and centred around the fundamental right for all individuals to maintain sovereignty over their personal information and data, and control over how their data is accessed and utilised. Our first preference to achieve this recommendation is to not release or share any personal individual information. If this first preference is not agreeable, the second preference is that this fundamental human right extends to building processes into the DAT Bill that provide for tangible mechanisms for individual's right to opt-in, access, amend, and control the storage and use of their personal information and data.

The DAT Bill and associated legislative instruments should require increased responsibilities on public and private sector agencies to strengthen the quality of fit for purpose data

acquisition in their data management practices. Only collecting data strictly relevant to the intended purpose of such data collection, and gaining informed, explicit, user-friendly consent at each stage of data collection and use from all individuals involved will better facilitate public trust and efficient processes. Accompanying this there must be significant disincentives and/or penalties for data misuse and non-compliance built into the DAT Bill. We recommend free access to justice and compensation provided to individuals who have had any damage (regardless of the perceived seriousness or potential for harm) caused due to privacy breaches be built into the DAT Bill.

Ethics

Balancing the benefits to the Australian public, economy, and governmental processes with the risk of breach of privacy and harm to individuals, particularly our most marginalised populations must not be overlooked. At all times, the Australian government is charged with protecting its citizens, and particularly its most vulnerable citizens. We respectfully advocate for the ethics processes to be significantly strengthened in consideration and upholding of all Australian individuals' fundamental human right to privacy and sovereignty over their own personal information.

Section 16 Data Sharing Principles Subclause (1)(a) requires observance of applicable ethics processes.[11] This includes, for example, observance of established academic ethics approval processes, and seeking independent advice on the ethical implications of sharing as appropriate. Use of ethics processes help ensure research and other projects have beneficial results while minimising risk of harm to relevant people, including data subjects.

We recommend that the use of formal ethics processes (such as those set out by the NHMRC) are mandatory in situations of sharing individuals' private data, rather than determined on a case by case basis and potentially non-compulsory. They are necessary for the impartial assessment of risk and the protection of Australian individuals' personal data. Additionally, we agree with the Privacy Impact Assessment recommendation that there needs to be a more specific framework outlined in the DAT Bill (preferably) or the DAT Bill Explanatory Memorandum (secondly) for guidance on ethics process requirements. This would include how the ethics processes interact with existing provisions in the Privacy Act. We do not believe this further detail should only be included in a guidance document, it must be inbuilt into the Bill itself or the Explanatory Memorandum.

The Privacy Impact Assessment recommendation states: "Specify, in supporting guidance material, when and how a Data Scheme Entity should undertake an ethics process and the nature of the process required. Possible circumstances to consider include cases:

- Involving sensitive information
- Where seeking consent is impracticable or unreasonable
- When it is not possible to use de-identified data
- Where the sharing would have a commercial application for the Accredited User
- Where there may be community concern about the proposed sharing."[12]

We strongly recommend that sensitive information must not be included in the DAT Bill as data that is eligible to be shared; seeking consent for releasing personal or sensitive

[11] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Data Availability and Transparency Bill 2020 Exposure Draft*

[12] Information Integrity Solutions, *Privacy Impact Assessment – Draft Data Availability and Transparency Bill 2020*

information is always mandatory; identified or re-identifiable data must not be included in the DAT Bill as eligible to be shared; and sharing data must not cause a commercial gain or profit for the user. If, however, the Office of the National Data Commissioner proceeds with the DAT Bill allowing sharing of sensitive, identifiable personal information without seeking consent from individuals, that may lead to a commercial gain for data users, then we strongly recommend that a formal ethics process must be undertaken in all potential data sharing projects of these natures.

Consent

The term 'consent' in the draft DAT Bill would take its ordinary meaning and would align with the Privacy Act and the APP Guidelines. The Guidelines state that valid consent has the following elements:

- The individual is adequately informed before giving consent
- The individual gives consent voluntarily
- The consent is current and specific, and
- The individual has the capacity to understand and communicate their consent.[13]

We assert that neither the Privacy Act, nor the DAT Bill, standards of consent meet the above conditions in terms of implementation and compliance monitoring. The gaining of consent by government agencies in Australia has long been insufficient and does not adequately safeguard individuals' privacy.

If personal or sensitive information is to be shared under the DAT Bill, we believe consent should be a mandatory requirement, as would be expected by public opinion. We recommend strengthening privacy provisions in the Privacy Act, as well as legislating within the Privacy Act and the DAT Bill requirements for gaining fully informed, easily-understood, freely-given consent during any data gathering processes. This includes strengthening initial consent requirements that are currently insufficient to ensure fully-informed, explicit, freely-given, and user-friendly consent, and re-obtaining consent from individuals any time an amendment in purpose for use of data or data sharing is requested or processed. This is particularly important for individuals who may not speak English as their primary language, have cognition-based impairments, have limited access to information, support or IT literacy to access or amend information gathered about them.

Section 16(1)(b) of the DAT Bill states that, where the data being shared includes personal information, consent for sharing is to be sought from the individuals concerned unless it is unreasonable or impracticable for the data scheme entities to do so.[14] According to the Explanatory Memorandum the 'unreasonable or impracticable' language is drawn from section 16A of the Privacy Act, and should be interpreted using relevant guidance on consent made by the Australian Information Commissioner.

The terms 'unreasonable or impracticable' within the context of 16A of the Privacy Act offers little to no guidance on how these terms should be interpreted within the DAT Bill. The language is contained within a two pronged test which includes assessing whether the entity reasonably believes the disclosure is necessary to 'lessen or prevent a serious threat to the

[13] Information Integrity Solutions, *Privacy Impact Assessment – Draft Data Availability and Transparency Bill 2020*

[14] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Data Availability and Transparency Bill 2020 Exposure Draft*

life, health or safety of any individual, or to public health or safety.'[15] The Office of the Australian Information Commissioner offers some examples, which all draw on the need to balance the unreasonableness or impracticality of gaining consent with the threat to life, health or safety of an individual, which is not relevant within the context of the DAT Bill.

The Explanatory Memorandum of the DAT Bill states that the question of whether seeking consent is reasonable or impracticable may depend on the amount, nature, and sensitivity of the data involved, and whether individuals gave informed consent for uses including the proposed sharing at the point the data was originally collected. Where it is unreasonable or impracticable to seek consent, parties must still consider implementing other controls to protect privacy, under this and other data sharing principles. This would indicate that the unreasonable or impracticable test within the DAT Bill is of a far lower threshold than the test put forward within the Privacy Act. Further guidance as to the circumstances that may be considered 'unreasonable or impracticable' must be specified within the DAT Bill, due to the incompatibility of section 16A of the Privacy Act and section 16(1)(b) of the DAT Bill currently referenced in the Explanatory Memorandum.

We note that the Privacy Impact Assessment states: "The combination of service delivery and direct contact with the individuals concerned would on its face make it difficult to see why consent would not be a feasible option to authorise sharing the information to provide services to them."[16] They go on to note a range of issues with privacy notices and privacy collection statements: "Many of the usual collection (APP 5) notices would not provide either sufficient or clear information to allow individuals to make informed choices about data sharing for government service." We affirm the recommendations in the Privacy Impact Assessment to provide specific guidance in the DAT Bill (not in separate, unenforceable guidelines) matters relating to how consent operates in the data sharing scheme to guide strong, appropriate models of consent.

We also affirm the IIS recommendation to develop and publish a regulatory action plan that outlines the National Data Commissioner approach to the oversight and enforcement of its powers and address how the Commissioner will monitor the data sharing scheme consent practices.

Aboriginal and Torres Strait Islander people's data

The DAT Bill consultation paper states: "The Bill will support the data policies developed by the National Indigenous Australians Agency and require users to adhere to applicable policies and processes when sharing and using data about Aboriginal and Torres Strait Islander peoples. All relevant ethics processes under current arrangements, such as the Australian Institute of Aboriginal and Torres Strait Islander Studies (AIATSIS) Code of Ethics – Guidelines for Ethical Research in Australian Indigenous Studies, will continue to apply and will need to be considered under the Project Principle to demonstrate the public interest of a given project. Similarly, data custodians and users could apply the CARE Principles when designing data governance systems as part of applying the safeguards under the Bill."[17]

[15] *The Privacy Act 1988* (Cth), Section 16A

[16] Information Integrity Solutions, *Privacy Impact Assessment – Draft Data Availability and Transparency Bill 2020*

[17] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Data Availability and Transparency Bill 2020 Exposure Draft Consultation Paper*

There is, however, not a single mention in the DAT Bill, the DAT Bill Explanatory Memorandum, nor the Regulations to Aboriginal and Torres Strait Islander peoples and specific data policies relating to these populations. We recommend stringent and appropriate data protection principles and policies written into the DAT Bill or the DAT Bill Explanatory Memorandum to safeguard Aboriginal and Torres Strait Islander peoples' sovereignty over their personal and sensitive information.

Data sharing agreements

Section 18 Data Sharing Agreement outlines the operations of Data Sharing Agreements under the Bill. Item 2 of the requirements for data sharing agreement requires agreements to specify that sharing is to be done under the DAT Bill. This makes intent to use the data sharing scheme clear on the face of the agreement, as necessary for the operation of the Bill's penalty provisions (refer to clause 14). Item 2 interacts with item 5, which requires parties to identify other applicable laws, such as those authorising the initial collection of the public sector data to be shared, and any secrecy or non-disclosure provisions to be overridden by the operation of the DAT Bill. These items ensure parties are aware of their legal responsibilities and liabilities in relation to sharing the data.

We agree with the Privacy Impact Assessment that: "Specifying the matters that Agreements must cover in the draft DATB helps to counteract that risk. Involvement of the NDC will also help get the balance right when setting expectations for the form and content of Data Sharing Agreements. The effectiveness of Data Sharing Agreements directly correlates with the effectiveness of privacy protections associated with the Scheme. IIS therefore encourages the NDC to monitor the form and content of Data Sharing Agreements and intervene to ensure they comply with the requirements and spirit of the Draft DATB."[18] The DAT Bill must be more specific in the requirements of what constitutes a Data Sharing Agreement, outlining approved and required content and legislating the responsibilities of the NDC with regard to the monitoring of the Data Sharing Agreements.

Transparency and oversight

We commend the DAT Bill for the inclusion of a range of transparency and oversight mechanisms, including the public register of all shared datasets and accredited users, as well as the regulatory powers of the National Data Commissioner to monitor and enforce compliance with the Bill. We recommend the following further transparency and oversight mechanisms be inbuilt into the DAT Bill:

- Automatic notifications sent to individuals when their data is used, shared, or released if their information forms part of a dataset (whether identification is possible or not)
- Notifications sent to individuals when their personal and/or sensitive data is breached, regardless of whether or not the breach would be likely to result in serious harm as required under section 26WE of the Privacy Act
- Accredited users must not include individuals, organisations, or entities that will be utilising the data released or shared for commercial gain, and
- Free and simple pathways to access justice and compensation provided to individuals who have had damage caused due to a privacy breach, not merely relying on the existing complaint mechanisms for data scheme entities. We agree with the Privacy Impact Assessment that "data sharing will take place in a complex system and individuals should not need to understand the system to have any issue

[18] Information Integrity Solutions, *Privacy Impact Assessment – Draft Data Availability and Transparency Bill 2020*

resolved. In addition, the diffuse accountability in the Data Sharing Scheme should not result in harm to individuals not being remediated because each party points at the other parties. Part of the ecosystem governance that the NDC is established to provide (along with the OAIC) must be to ensure remediation happens."[19] It is inconsistent to have individuals complain through the OAIC under the *Privacy Act*, while allowing data scheme entities to complain directly to the NDC, the Commissioner with regulatory oversight under the draft bill. This ignores the important fact that it is individual's data that may be shared under the bill. The bill should allow both individuals and data scheme entities to complain to the NDC about non-compliance under Part 5.3.

Additionally, we support the recommendation made by The National Association of People with HIV Australia (NAPWHA) and Scarlet Alliance's submission that Part 3.3 of the DAT Bill must go further in addressing data breaches. In particular, that an addition into Part 3.3 should be made to require all data scheme entities to report to the Commissioner any actual or suspected data breaches, regardless of the perceived seriousness or potential for harm. The Commissioner must then make a public disclosure of all data breaches, ensuring enhanced transparency and accountability under the DAT Bill. We agree that these additional requirements are an opportunity to improve the data sharing scheme and facilitate increased confidence in the management procedures.

Evaluation

The DAT Bill consultation paper states that: "The Bill, legislative instruments, Guidelines, and guidance will be reviewed periodically to ensure the data sharing scheme operates as intended, and to provide an opportunity for improvement. As a new scheme impacting data across government, the Bill will be reviewed three years after commencement which could assess its effectiveness. Periodic reviews will then occur every ten years from commencement to address emerging issues, with reports to be tabled in Parliament."[20] We assert that the evaluation framework must be inbuilt into the DAT Bill or the DAT Bill Explanatory Memorandum prior to implementation of the Bill, and should be in the form of an evaluation of the outcomes from development and implementation of the Bill, the data which is publicly available with a mechanism to allow for amendment of the Bill when evaluated, showing the net costs of the new legislation in comparison to the benefits received by the Australian public.

We agree with the Privacy Impact Assessment's assertion that: "For a piece of law with such potential to impact on the amount of information about individuals that is shared for new purposes, the number of parties that could be involved in data sharing and given the rapidly changing nature of the technological and social environment in which data sharing will occurs, IIS considers the review periods (seven years after the initial review, and every ten years thereafter) to potentially be too infrequent. While the risk of obsolescence is reduced due to the DATB's principles-based approach and the NDC's ability to make codes and issue guidelines, there is nevertheless the possibility that the Act's privacy protections will no longer be fit-for-purpose and require updating within the span of 10 years."[21] We recommend

[19] Information Integrity Solutions, *Privacy Impact Assessment – Draft Data Availability and Transparency Bill 2020*

[20] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Data Availability and Transparency Bill 2020 Exposure Draft Consultation Paper*

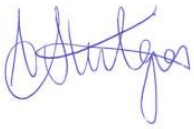
[21] Information Integrity Solutions, *Privacy Impact Assessment – Draft Data Availability and Transparency Bill 2020*

that the evaluation period be written into the DAT Bill of initial review three years after implementation, and every five years thereafter.

Furthermore, Positive Life and HALC support the comments and recommendations in the additional submission to the Office of the National Data Commissioner made by NAPWHA and Scarlet Alliance.

If additional information or citations in relation to this submission are required, please feel free to contact Jane on janec@positivelife.org.au or Alex on alexs@halc.org.au.

Yours sincerely,



Jane Costello
Chief Executive Officer
Positive Life NSW

Alex Stratigos
Principal Solicitor
HIV/AIDS Legal Centre

The following organisations support the statements and recommendations provided to the Office of the National Data Commissioner in this Positive Life NSW and HIV/AIDS Legal Centre submission: The National Association of People with HIV Australia, Positive Life South Australia, Positive Lives Tasmania, Queensland Positive People, and Positive Organisation Western Australia