APPENDIX 3: The policy and legal framework underpinning this Framework

The system of privacy regulation in Australia is best described as 'patchwork'. Given the range of current and potential future SynD members, a range of privacy laws may apply to a single synthetic health data project.

Federal government agencies and private sector organisations are generally regulated by the Australian Privacy Principles (APPs), which are found in the federal *Privacy Act 1988* (Cth).[25]

State/Territory and local government agencies, including public universities, are generally regulated by their own State/Territory privacy laws. Some States/Territories have multiple privacy laws and sets of privacy principles. For example, NSW has the Information Protection Principles (IPPs) set out in the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) and the Health Privacy Principles (HPPs) set out in the *Health Records & Information Privacy Act 2002* (NSW) (HRIP Act). However, some States – such as South Australia – do not have any specific privacy laws regulating either State or local government agencies.

Some private sector organisations will be regulated by *both* federal and State/Territory privacy laws. For example, the HRIP Act applies the NSW HPPs to private sector health service providers, in addition to the federal APPs.

Each privacy law contains a set of privacy principles, each of which covers similar ground, regulating the collection, use and disclosure of 'personal information' (or a sub-set of personal information, such as 'health information' or 'sensitive information'), as well as data security, data quality, access and correction rights. As a very general statement, privacy laws typically prohibit the disclosure of personal information, unless an exception applies.

The privacy laws that apply to SynD organisations (both current and future) could include:

Commonwealth privacy laws

- the *Privacy Act 1988* (Cth) (Privacy Act)[26]

The Privacy Act applies to Commonwealth government agencies (including Commonwealth public universities) and private sector organisations. This includes all private sector and NGO health service providers across Australia.

[25] There is an exemption for private sector organisations with a turnover of less than $3M pa, but this exemption does not apply to 'health service providers'. This means that even very small NGO and community organisations which offer health services will therefore be regulated by the APPs.
[26] See: https://www.legislation.gov.au/C2004A03712/latest/text

Australian Capital Territory

- the *Information Privacy Act 2014* (ACT) (IP Act),[27] and
- the *Health Records (Privacy and Access) Act 1997* (ACT) (HRPA Act)[28]

The IP Act applies to ACT public sector agencies (including ACT public universities) and sets out 13 Territory Privacy Principles (TPPs).

The IP Act does not apply to the handling of 'health information' about individuals, which is instead regulated by the HRPA Act.

The HRPA Act applies to both public sector and private sector health service providers and contains 12 Privacy Principles (PPs).

New South Wales

- the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act),[29] and
- the *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act)[30]

NSW public sector agencies (including NSW public universities) must comply with the PPIP Act which has 12 Information Protection Principles (IPPs) and the HRIP Act which has 15 Health Privacy Principles (NSW HPPs). The HRIP Act also applies to all private sector health service providers.

Northern Territory

- the *Information Act 2002* (NT) (Information Act)[31]

Northern Territory public sector agencies (including NT public universities) must comply with the IP Act, which contains 10 Information Privacy Principles (NT IPPs).

Queensland

- the *Information Privacy Act 2009* (QLD) (IP Act)[32]

[27] See: https://www.legislation.act.gov.au/View/a/2014-24/current/html/2014-24.html
[28] See: https://www.legislation.act.gov.au/View/a/1997-125/current/html/1997-125.html
[29] See: https://legislation.nsw.gov.au/view/html/inforce/current/act-1998-133
[30] See: https://legislation.nsw.gov.au/view/html/inforce/current/act-2002-071
[31] See: https://legislation.nt.gov.au/Legislation/INFORMATION-ACT-2002
[32] See: https://www.legislation.qld.gov.au/view/whole/html/speciallabel/bill-2022-041/act-2009-014 (this version of IP Act indicates the amendments that will be made by the IPOLA Act)

The IP Act contains 13 Queensland Privacy Principles (QPPs). Queensland government agencies (including Queensland public universities) must comply with the QPPs.

South Australia

There are no specific privacy laws in South Australia. However, the Department of Premier and Cabinet has issued a privacy Instruction for South Australian public sector agencies (Premier and Cabinet Circular 12 - Information Privacy Principles Instruction)[33]. The Instruction contains 10 Information Privacy Principles (SA IPPs) which apply to the handling of personal information. The Instruction was last re-issued in May 2020.

While the Instruction creates a binding policy for public sector agencies, it is not law and cannot be enforced by a court. The Instruction creates the Privacy Committee of South Australia, which handles privacy complaints relating to the SA IPPs.

Tasmania

- the *Personal Information Protection Act 2004* (Tas) (PIP Act)[34]

Tasmanian public sector agencies (including Tasmanian public universities) are required to comply with the PIP Act, which has 10 Personal Information Protection Principles (PIPPs).

Victoria

- the *Privacy and Data Protection Act 2014* (Vic) (PDP Act),[35] and
- the *Health Records Act 2011* (Vic) (HR Act)[36]

Victorian public sector agencies (including Victorian public universities) must comply with the PDP Act, which has 10 Information Privacy Principles (IPPs) and with the HR Act which has 11 Health Privacy Principles (Vic HPPs).

Private sector health service providers are also required to comply with the HR Act.

[33] See: https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf
[34] See: https://www.legislation.tas.gov.au/view/whole/html/asmade/act-2004-046
[35] See: https://www.legislation.vic.gov.au/in-force/acts/privacy-and-data-protection-act-2014/031
[36] See: https://www.legislation.vic.gov.au/in-force/acts/health-records-act-2001/049

Western Australia

- the *Privacy and Responsible Information Sharing Act 2024* (WA) (PRIS Act)[37]

Until very recently, Western Australia did not have comprehensive privacy legislation to regulate how the WA public sector handles personal information. At this stage, it is anticipated that the privacy provisions in the PRIS Act will commence in 2026.[38]

The PRIS Act creates 11 Information Privacy Principles (WA IPPs) that apply to the handling of personal information (including health information) by WA public sector organisations (including WA public universities).

The PRIS Act also creates a responsible information sharing legislative framework that governs the handling of WA government data. Under this Framework, information sharing agreements can be formed under the terms of the PRIS Act, giving legal authority for the collection, use and disclosure of government information.[39] These agreements may be made between WA public entities and other parties – either other WA public entities or external entities.

Other relevant laws

Organisations may also be subject to other laws that impact data handling. These laws typically govern specific functions or services of an organisation, and can guide the collection, use, disclosure and management of personal information. An example of a law governing a specific function or service would include the *Public Health Act 2010* (NSW).

Other relevant policies

SynD members may also have their own policies that apply to the creation and handling of synthetic health data. These policies will need to be applied by these organisations alongside this Framework where a synthetic health data request is within scope of this Framework.

[37] See: https://www.legislation.wa.gov.au/legislation/statutes.nsf/law_a147470.html
[38] News story: Interim advice for all agencies about the protection of personal information, 9 December 2024, accessible at https://www.wa.gov.au/government/announcements/interim-privacy-position-0
[39] See Part 3, Division 5, PRIS Act.

Summary of applicable Australian privacy laws that regulate the handling of health information**

Where privacy laws establish specific obligations for the handling of 'health information' or 'sensitive information' (as a distinct category of 'personal information') – either through separate legislation or a specific set of privacy principles – these are the relevant privacy obligations that will apply to the handling of health data. Other non-privacy laws may also impact the handling of health information.

Organisation	**Privacy Act/APPs**	**ACT HRPA Act/PPs***	**NSW HRIP Act/HPPs***	**NT IP Act/IPPs***	**QLD IP Act/QPPs***	**SA Privacy Instruction/ IPPs***	**TAS PIP Act/PIPPs***	**VIC HR Act/HPPs***	**WA PRIS Act/IPPs***
Private sector health service providers (e.g. GPs, private hospitals)	Y	Y	Y	N	N	N	N	Y	N
Health NGOs (e.g. PHNs)	Y	Y	Y	N	N	N	N	Y	N
State/Territory public sector agency (e.g. public hospitals, state public universities)	N	Y	Y	Y	Y	Y	Y	Y	Y
Commonwealth government agencies (e.g. Department of Health, Disability and Ageing)	Y	N	N	N	N	N	N	N	N

* If operating in the State or Territory

** Where Entity A engages Entity B as a 'contracted service provider', the privacy laws that apply to Entity A may then also apply to Entity B.