

Direction under section 62(1) of the *Health Records and Information Privacy Act 2002 (NSW)* in relation to the “Their Futures Matter” project

As Privacy Commissioner appointed under Part 4, Division 1 of the *Privacy and Personal Information Protection Act 1998 (NSW)* I, Samantha Gavel, hereby direct pursuant to section 62(1) of the *Health Records and Information Privacy Act 2002 (NSW)* (the **HRIP Act**) that:

Overview

1. This is a Direction made under section 62(1) of the HRIP Act. It should be read in conjunction with the HRIP Act.

Interpretation

2. In this Direction, unless the contrary intention appears, the following words have the respective meanings set out below:

“**Analytical Services**” means the study, analysis, modelling, research or evaluation of Tier Two Data.

“**Approved Analyst**” means the Project Team or a person (including a researcher or analyst) that:

- a) has been approved by the Project Team to provide Analytical Services for and on behalf of the Project Team; and
- b) is under a contractual obligation to comply with the HRIP Act to the extent modified by this Direction.

“**Approved Purpose(s)**” has the meaning given in paragraph 9 of this Direction.

“**Chair**” means the Secretary of the NSW Department of Family and Community Services.

“**Children**” means persons under the age of 16 years.

“**Data Analytics Entity**” means a data analytics entity or function that is operated by a Public Sector Agency that is compliant with the current NSW Government Digital Information Security Policy, and that is engaged by the Project Team to undertake Analytical Services for the Project, such as the DAC (as defined in section 4 of the *Data Sharing (Government Sector) Act 2015 (NSW)*) or such other entity that is under a contractual obligation to comply with the HRIP Act to the extent modified by this Direction.

“**Data Linkage Centre**” means a data linkage service or function that is operated by a Public Sector Agency that is compliant with the current NSW Government Digital Information Security Policy, and that is engaged by the Project Team to undertake data linkage for the Project, such as the Centre for Health Record Linkage or such other entity that is under a contractual obligation to comply with the HRIP Act to the

extent modified by this Direction.

“Direction” means this direction, including Schedule 1.

“Health Information” has the meaning given in section 6 of the HRIP Act and includes the information set out in Part A of Schedule 1 of this Direction.

“Health Service” has the meaning given in section 4(1) of the HRIP Act.

“HPP(s)” means the health privacy principles, which are contained in Schedule 1 of the HRIP Act.

“HRIP Act” means the *Health Records and Information Privacy Act 2002* (NSW).

“Human Services Data” means data or information (which may include Health Information) within a Participating Agency's or its contractors' or agents' records or systems in connection with a Public Sector Agency's or other government agencies' interactions with, or provision of supports, services or programs to, an individual.

“Identifier Information” has the meaning given in paragraph a.i. in Part A of Schedule 1.

“Information Protection Gates” means the privacy verification process and checks that will be undertaken by the Data Analytics Entity or an Approved Analyst in accordance with this Direction and before information held by the Data Analytics Entity or an Approved Analyst is externally released or disclosed to:

- a) ensure compliance with this Direction;
- b) ensure that only de-identified information is released or disclosed to a third party; and
- c) prevent re-identification of information by a third party, including a Participating Agency.

“Participating Agency” means a Public Sector Agency that collects or holds Human Services Data that is relevant to the Project and which has agreed to participate in the Project by disclosing Human Services Data to the Data Linkage Centre in accordance with this Direction.

“Personal Information” has the same meaning as in section 5 of the HRIP Act.

“PPN” means a project specific person number that the Data Linkage Centre allocates to individuals whose Health Information is collected and used as part of the Project for privacy purposes and to help prevent re-identification of those individuals.

“Project” means the “Their Futures Matter” project as described in paragraphs 4 to 6 of this Direction.

“Project Cohort” means individuals born on or after 1 January 1990 (**Primary Project Cohort**) and individuals relevant to or related to those individuals; for example, family members, relatives, guardians and carers (**Secondary Project Cohort**).

Cohort).

“Project Objectives” means the study, analysis, research and evaluation of government service design and delivery in connection with the provision of supports, services and programs to Vulnerable Children or Young Persons in order to meet the objectives described in paragraphs 4 and 6 of this Direction.

“Project Team” means the team established by the NSW Government to coordinate and lead the Project. The Project Team may include authorised representatives from certain Participating Agencies.

“Protection System” means the system for the protection or care of Children or Young Persons that is provided or facilitated by a Public Sector Agency or other government agency, such as the NSW Department of Family and Community Services.

“Public Sector Agency” has the meaning given in section 4(1) of the HRIP Act.

“Service Usage Data” has the meaning given in paragraph c.i. in Part B of Schedule 1.

“Tier One Data” means Human Services Data that has not been through any de-identification process to remove any Health Information.

“Tier Two Data” means data derived from Tier One Data that has had Identifier Information removed and been allocated a PPN in accordance with this Direction.

“Tier Three Data” means aggregated Tier Two Data that has been through the Information Protection Gates process in accordance with this Direction.

“Vulnerable Children or Young Persons” means Children, Young Persons or young adults who are within the Primary Project Cohort and who:

- a) are part of a family who is, or may be, at a social or economic disadvantage;
- b) are at a disadvantage by reason of trauma, disability or cognitive impairment;
- c) are, have been, or are at a reasonable risk of coming into contact with the Protection System because of their circumstances; or
- d) are the alleged victim or alleged perpetrator of a crime.

“Young Persons” means persons who are aged 16 years or above but who are under the age of 18 years.

Application

3. Unless otherwise specified, this Direction applies to Participating Agencies and to certain other Public Sector Agencies to the extent set out in this Direction.

Project Objectives

4. The Project is known as “Their Futures Matter”. This Direction has been prepared to

facilitate the Project Objectives. The Project Objectives are to help ensure that effort and funding across government is focussed on interventions that will improve the long-term outcomes for Vulnerable Children or Young Persons and their families at the earliest opportunity. To this end, the Project will use extensive Human Services Data from across government to design and deliver better government services for Vulnerable Children or Young Persons and their families.

5. The Project will use three different types of datasets that are derived from the Human Services Data. Data is allocated a different tier depending on what stage of the data de-identification and verification process it has been through.
6. The data that is collected and used as part of the Project will:
 - 6.1 provide specific identifications of trends and gaps in government service usage and delivery;
 - 6.2 facilitate services that are better tailored to the needs of Vulnerable Children or Young Persons and their families both now and in the future;
 - 6.3 deliver clear evidence on service, support and program effectiveness and a detailed view of resource allocation and gaps;
 - 6.4 provide valuable information for research and planning of government supports and services; and
 - 6.5 enable Participating Agencies and other government agencies to meet the Project Objectives by implementing new policy and program development directed to improving outcomes for Vulnerable Children or Young Persons and their families.

Scope of Direction

7. This Direction has been made to:
 - 7.1 permit Participating Agencies to disclose Tier One Data relating to persons in the Project Cohort, or which is reasonably relevant to the Project, to the Data Linkage Centre; and
 - 7.2 permit the Data Linkage Centre to collect this Tier One Data so it may link the data with other datasets and generate a PPN for the Approved Purposes.
8. This Direction recognises that:
 - 8.1 the Data Analytics Entity's and Approved Analysts' role is to:
 - a) collect and analyse the Tier Two Data for the Approved Purposes; and
 - b) verify and check that no Health Information was included in any Tier Two Data that it collected and does not form part of any Tier Three Data that is disclosed to any third party as part of the Project; and
 - 8.2 Participating Agencies, Public Sector Agencies, the Project Team and other third parties, such as universities and researchers may have access to and use of Tier Three Data,
to the extent set out in this Direction.
9. The Approved Purposes means any activity, task, work, step, process or measure that facilitates or enables the Project Objectives (**Approved Purposes**).
10. The Data Linkage Centre, Data Analytics Entity and an Approved Analyst must not

use any data derived from the Human Services Data, which is disclosed by a Participating Agency to the Data Linkage Centre, if that purpose is not for the Project and for an Approved Purpose(s).

11. Under no circumstances may any information that is collected as part of the Project be used to target an individual to receive specific supports, services, programs or other forms of government intervention.
12. Entities and persons that provide Analytical Services must keep Tier Two Data confidential, secure and protected from unauthorised use and disclosure in accordance with this Direction.
13. Once data is Tier Two Data or Tier Three Data, no entity or person may re-identify or cause any data collected as part of the Project to be re-identified by any means, except as part of the Information Protection Gates process conducted by the Data Analytics Entity or an Approved Analyst. If re-identification is found to have occurred, whether deliberately or inadvertently, the Chair must notify the NSW Privacy Commissioner within 48 hours of the Chair confirming that such re-identification has occurred, except where the re-identification was by the Data Analytics Entity or an Approved Analyst as part of the Information Protection Gates process.
14. I am satisfied that the public interest in making this Direction is greater than the public interest in requiring the Participating Agencies to comply with the HPPs.
15. A corresponding direction applies in respect of “personal information” within the meaning of section 4 of the *Privacy and Personal Information Protection Act 1998* (NSW).

Flows of Health Information

16. The Health Information flows that will occur as part of the Project are set out in Part B of Schedule 1. In summary, the below process will occur.

Provision of Tier One Data to the Data Linkage Centre

17. Participating Agencies will need to provide Tier One Data about individuals within the Project Cohort to the Data Linkage Centre for the purposes of data or record linkage and to distinguish between individuals.
18. In addition, if, after taking reasonable steps to do so, Participating Agencies cannot accurately identify individuals within the Project Cohort, they may provide Tier One Data that they hold, and which is reasonably relevant to the Project, to the Data Linkage Centre. That Tier One Data will be filtered by the Data Linkage Centre to identify persons within the Project Cohort. Health Information from individuals outside the Project Cohort will be retained for no longer than is necessary for determining whether or not an individual is within the Project Cohort. The Health Information of persons determined to be outside the Project Cohort will be disposed of securely in accordance with HPP 5(1)(b) and the Project governance framework.
19. Participating Agencies will also periodically update the Tier One Data that they supplied to the Data Linkage Centre to help ensure that it remains relevant, up-to-date, accurate and is a longitudinal, evolving and more complete dataset. Participating Agencies will do so by providing the updated data to the Data Linkage Centre.

20. Participating Agencies will only provide Tier One Data to the Data Linkage Centre where the Tier One Data has previously been lawfully collected by the relevant Participating Agency in accordance with the HRIP Act or with other lawful authorisation. By way of example, if a Participating Agency lawfully collected Tier One Data for purpose Y (including with all necessary consents and notices) (**Initial Collection**), even though consent may not have been obtained in relation to the Project and the Approved Purposes, under this Direction the Participating Agency may disclose the information collected as part of the Initial Collection to the Data Linkage Centre in accordance with this Direction. This is because the information has previously been lawfully collected by the relevant Participating Agency (that is, for purpose Y).

Collection and use of Tier One Data by the Data Linkage Centre

21. The Data Linkage Centre will collect Tier One Data from Participating Agencies for the purposes of data linkage and to allocate a PPN. Once Tier One Data has been through this process, it will become Tier Two Data.

Collection and use of Tier Two Data by the Data Analytics Entity or an Approved Analyst

22. The Data Linkage Centre will provide Tier Two Data to the Data Analytics Entity and to Approved Analysts to provide Analytical Services and other data services set out in this Direction.
23. The Data Analytics Entity and Approved Analysts will pass the Tier Two Data through the Information Protection Gates to ensure that no Health Information was included in any Tier Two Data and that no Health Information is externally released. As part of the Information Protection Gates process, the Data Analytics Entity and Approved Analysts will adopt best practice privacy, security and de-identification practices, including compliance with the NSW Government Digital Information Security Policy. If required they may also adopt “confidentialisation” in accordance with the Australian Bureau of Statistics’ Confidentiality Information Series. Confidentialisation will be required where an individual exhibits uncommon or unique traits that may allow them to be indirectly or directly identified based on specific datasets.
24. Once Tier Two Data has successfully passed the Information Protection Gates process, it will become Tier Three Data. Tier Three Data will include the results, findings, insights and other de-identified information derived from the analysis of the Tier Two Data. Tier Three Data will not contain any Health Information.

Disclosure of Tier Three Data

25. The Data Analytics Entity and Approved Analysts may disclose Tier Three Data to researchers, universities, the Project Team, Participating Agencies and Public Sector Agencies. They may also make certain Tier Three Data publicly available.
26. It is important to note that before any results, findings or other information that may have been derived from the Human Services Data is externally released to the public it needs to pass the Information Protection Gates to help ensure that it has been sufficiently de-identified such that it no longer falls within the definition of Health Information under section 6 of the HRIP Act. This requirement will limit any privacy impacts in respect of individuals and will help ensure that only Tier Three Data is ever made publicly available.

Authority to collect, use and disclose Health Information in connection with the Project

27. To protect the privacy of individuals, information about persons collected as part of the Project will only be collected, used and disclosed as described in this Direction.
28. Only limited and authorised personnel within Participating Agencies and Public Sector Agencies, and with appropriate delegation, will have the authority to collect, use and disclose Health Information in connection with the Project. All entities and persons that may be provided with Health Information will be subject to privacy and confidentiality obligations to protect it from unauthorised use and disclosure.
29. It is recognised that in some cases contractors or agents will act on behalf of Participating Agencies and Public Sector Agencies. The authority to collect, use and disclose Health Information in connection with the Project may, in appropriate cases, be delegated by Participating Agencies or other Public Sector Agencies to their agents and contractors, subject to them being contractually bound to comply with the same privacy and security obligations that Participating Agencies and other Public Sector Agencies are required to comply with at law and under this Direction.

Custody and control of Human Services Data

30. Once Human Services Data is collected by the Data Linkage Centre, the Chair will have overriding custodianship, control of and responsibility for that data. The Chair will be responsible for ensuring compliance with this Direction and for notifying of any contraventions of this Direction in accordance with paragraph 35 of this Direction.

Access to Human Services Data

31. If an individual makes a request to the Data Linkage Centre to access Health Information that has been collected by the Data Linkage Centre as part of the Project, the Data Linkage Centre will refer the request to the relevant Participating Agency that originally supplied the Human Services Data, which included the relevant Health Information, to the Data Linkage Centre.

Exemption or modification to Health Privacy Principles

32. This Direction exempts or modifies the HPPs to the extent described below.

HPP	Exemption or modification sought to HPP
HPP 1 Purposes of collection of Health Information	Where the Data Linkage Centre collects Health Information in connection with the Project and for an Approved Purpose(s), it need not comply with HPP 1 where that Health Information has previously been lawfully collected in accordance with the HRIP Act (including where it has been originally collected for purposes unrelated to the Project and the Approved Purpose(s)).
HPP 2 Information must be relevant, not excessive, accurate and not intrusive	A Participating Agency need not comply with HPP 2 in relation to Health Information that has previously been lawfully collected in accordance with the HRIP Act, where that Health Information is subsequently disclosed to the Data Linkage Centre in connection with the Project and for an Approved Purpose(s).
HPP 3 Collection to be from individual concerned	Where the Data Linkage Centre collects Health Information in connection with the Project and for an Approved Purpose(s), it need not comply with HPP 3 where that Health Information has

HPP	Exemption or modification sought to HPP
	previously been lawfully collected in accordance with the HRIP Act (including where it has been originally collected for purposes unrelated to the Project and the Approved Purpose(s)).
HPP 4 Individual to be made aware of certain matters	<p>Where the Data Linkage Centre collects Health Information in connection with the Project and for an Approved Purpose(s), it need not comply with HPP 4 where that Health Information has previously been lawfully collected in accordance with the HRIP Act (including where it has been originally collected for purposes unrelated to the Project and the Approved Purpose(s)).</p> <p>A Participating Agency need not comply with HPP 4 in relation to Health Information that has previously been lawfully collected in accordance with the HRIP Act, where that Health Information is subsequently disclosed to the Data Linkage Centre in connection with the Project and for an Approved Purpose(s).</p>
HPP 5 Retention and security	No exemption from or modification to this HPP.
HPP 6 Information about Health Information held by organisations	The Data Linkage Centre that holds Health Information, need not comply with HPP 6, where the Health Information that it holds was collected by the Data Linkage Centre in connection with the Project and for an Approved Purpose(s).
HPP 7 Access to Health Information	The Data Linkage Centre that holds Health Information, need not comply with HPP 7, where the Health Information that it holds was collected by the Data Linkage Centre in connection with the Project and for an Approved Purpose(s).
HPP 8 Amendment of Health Information	The Data Linkage Centre that holds Health Information, need not comply with HPP 8, where the Health Information that it holds was collected by the Data Linkage Centre in connection with the Project and for an Approved Purpose(s).
HPP 9 Accuracy	<p>The Data Linkage Centre need not comply with HPP 9 where:</p> <ul style="list-style-type: none"> a) the entity that supplied the Health Information to it has warranted or is under a legal obligation to ensure the Health Information is accurate, up-to-date, complete and not misleading as at the date supplied; and b) the Health Information is to be used in connection with the Project, for an Approved Purpose(s) and in accordance with this Direction.
HPP 10	The Data Linkage Centre and a Participating Agency need not comply with HPP 10 and may

HPP	Exemption or modification sought to HPP
Limits on use of Health Information	use Health Information where the use is in connection with the Project, for an Approved Purpose(s) and in accordance with this Direction.
HPP 11 Limits on disclosure of Health Information	A Participating Agency need not comply with HPP 11 and may disclose Health Information that it holds to the Data Linkage Centre, where the disclosure is in connection with the Project, for an Approved Purpose(s) and in accordance with this Direction.
HPP 12 Identifiers	The Data Linkage Centre need not comply with HPP 12 and may assign an identifier to an individual and use or disclose such identifier in connection with the Project and for the Approved Purpose(s).
HPP 13 Anonymity	No exemption from or modification to this HPP.
HPP 14 Transborder data flows and data flow to Commonwealth agencies	No exemption from or modification to this HPP.
HPP 15 Linkage of Health Information	No exemption from or modification to this HPP.

33. It is the Data Linkage Centre that will in the majority of situations collect Health Information as part of the Project. Due to the use of a PPN, which will remove Identifier Information such as names and addresses, it is considered a remote possibility that any Health Information will be collected by the Data Analytics Entity or an Approved Analyst. If such information was collected by the Data Analytics Entity or an Approved Analyst, the risk of re-identification by a third party is mitigated through the Information Protection Gates. The Information Protection Gates are a quality assurance process that are designed to check and validate that no Health Information exists in any Tier Two Data and that only Tier Three Data (that is, data without any Health Information) is publicly released.
34. It is a condition of the granting of the above modifications and exemptions that all entities and persons involved in the Project protect Health Information in the manner required under HPP 5 and in accordance with this Direction.
35. Where any entity involved in the Project collects, uses or discloses Health Information other than in accordance with this Direction, the Chair must notify the NSW Privacy Commissioner within 48 hours of the Chair confirming that such a contravention has occurred.

Reporting and auditing

36. The Chair will report annually to the NSW Privacy Commissioner on compliance with this Direction, including the following matters:
 - 36.1 confirmation by the Chair regarding the correctness of any and all disclosures in connection with the Project;

- 36.2 the detail of any complaints received from the public regarding the Project;
 - 36.3 any circumstances where there has been any data breaches involving Health Information or where such breaches could have arisen; and
 - 36.4 the results of all audits conducted in accordance with paragraph 37.
37. The Project Team (or its authorised representative) will annually audit compliance with this Direction. As part of this process, the Project Team will audit and assess whether there are sufficient security systems and processes in place to protect Health Information that is collected, used and disclosed as part of the Project. The audit may involve the collection of audit reports from entities involved in the Project.

Duration

38. This Direction commences on the date signed by me and has effect for a period of three years from this date, or until a Code of Practice or legislative amendments are made to incorporate this Direction (whichever is earlier).
39. This Direction will be reviewed six months prior to its expiry.

Signed by me on the 13th of July 2018.



Samantha Gavel
NSW Privacy Commissioner

SCHEDULE 1

PART A: Health Information

The Health Information that may be collected as part of the Project may include:

- a. Personal Information collected to provide, or in providing, a Health Service to an individual, such as:
 - i. core identifying information, such as names and addresses (**Identifier Information**);
 - ii. personal characteristics of individuals, including sex, place of birth and languages spoken at home; and
 - iii. health service provider or hospital records (including hospital admission and discharge records);
- b. information or an opinion about the physical or mental health or disability of an individual;
- c. information or an opinion about an individual's express wishes about the future provision of a Health Service to him or her; and
- d. healthcare identifiers within the meaning of section 4(1) of the HRIP Act.

PART B: Summary of Health Information flows

The Project will involve the following process and associated information flows.

- a. A Participating Agency will identify that it has Tier One Data about an individual in the Project Cohort or which may be reasonably relevant to the Project.
- b. The Participating Agency's authorised representative will supply (through secure file transfer) Tier One Data about persons in the Primary Project Cohort (or which may be reasonably relevant to the Project) to the Data Linkage Centre. Tier One Data about individuals in the Secondary Project Cohort may also be supplied to the Data Linkage Centre. This information will be supplied in the same secure manner and at the same time or at a later date as the information about the subject individual.
- c. Tier One Data can be supplied to the Data Linkage Centre in two formats:
 - i. with Identifier Information separated from information in relation to a person's usage of, or interaction or engagement with, government supports, services and programs (**Service Usage Data**); or
 - ii. without Identifier Information separated from Service Usage Data.
- d. Where Identifier Information has been separated from Service Usage Data, the two datasets are received by different areas within the Data Linkage Centre and handled separately.
- e. Where Identifier Information has not been separated from Service Usage Data, the Data Linkage Centre undertakes the separation. The two datasets are then received by different areas within the Data Linkage Centre and handled separately.
- f. The Data Linkage Centre will replace Identifier Information with an arbitrary PPN. The result is a dataset that now constitutes Tier Two Data.
- g. The Data Linkage Centre will send Tier Two Data to the Data Analytics Entity by way of secure file transfer protocol.

- h. On receipt of the Tier Two Data, the Data Analytics Entity will review and cleanse the data for quality assurance purposes, including to ensure the usability and accuracy of the data. Using the PPN, the Data Analytics Entity will then join and update the submitted datasets with other datasets that may have previously been collected by the Data Analytics Entity for the same individual. This linked data will be collected, used and disclosed in accordance with the Direction.
- i. For the purposes of facilitating the Analytical Services, the Data Linkage Centre and the Data Analytics Entity may provide Tier Two Data to an Approved Analyst by way of secure file transfer protocol.
- j. The Data Analytics Entity or an Approved Analyst will complete Analytical Services on the Tier Two Data. At the completion of this process, the Data Analytics Entity or an Approved Analyst may make the results, findings and other information that may have been derived from the Tier Two Data available to third parties. All results, findings and information that are made available to third parties constitutes Tier Three Data. Tier Three Data has passed the Information Protection Gates prior to external release to help ensure that the information is de-identified and does not include any Health Information.

PART C: Privacy protections and controls

In developing the Project, the protection of privacy has been a paramount consideration. Stringent measures and controls have been built into the Project to protect the privacy of individuals and to mitigate potential privacy breaches. Some of those measures and controls are summarised below:

- a. allocating a PPN to individuals. For privacy purposes, each PPN is unique to the Project and the individual and does not follow a pattern such that it could be deciphered to identify a particular individual or class of individuals. Furthermore, the PPN is not generated from any aspect of the Health Information that it relates to, and therefore it is not associated with any Identifier Information;
- b. the use of Information Protection Gates;
- c. the use of secure systems and processes, including the use of secure file transfer protocol to transfer data to the Data Analytics Entity and an Approved Analyst;
- d. separating Identifier Information and Service Usage Data within the Data Linkage Centre. This separation creates a safeguard against identifying individuals and their recorded information outside the Participating Agency that holds the original record;
- e. ensuring that only limited and authorised persons can access Health Information in connection with the Project, which must be accessed with secure access controls and in compliance with this Direction;
- f. the implementation of a governance framework for the Project, which will include a framework for the protection of Health Information and a transparent process to request, handle and secure datasets;
- g. annual reporting and auditing requirements as set out in this Direction;
- h. compliance with, and audit against, all mandatory security requirements under legislation as well as several voluntary and best practice frameworks for security access and analysis, including strictly controlling individuals accessing or analysing data and prevention of any usage that is not in accordance with this Direction; and
- i. only permitting data that has at least reached the status of being Tier Two Data to be used for analysis by the Data Analytics Entity and an Approved Analyst in connection with the Project.