ASH NZ Data Access Policy for External Researchers

Updated August 2021

Acknowledgements

Action for Smokefree 2025 (ASH NZ) would like to acknowledge that this policy and related forms and documents have been largely based on the Te Hiringa Hauora/Health Promotion Agency data access protocols, as well as the data access protocols developed and used by Health and Disability Intelligence of the Ministry of Health.

ASH NZ would like to thank Health and Disability Intelligence and Te Hiringa Hauora for the time and effort that went into setting up their processes and in so doing, providing a template for ASH's processes to be based on that that encourages researchers to access the data, while protecting the privacy of those from whom the data were collected.

Contents

Acknowledgements 2
Introduction 4
Data Access Policy 5
    Principles 5
    General terms and conditions 7
Procedure 9
    How to apply for access 9
    The decision-making process 9
References 12
Appendix A – Relevant legislation, protocol, and guidelines 13
Appendix B – Statistics Act 1975 15
Appendix C – Official Statistics System (OSS) Protocols 15
Appendix D – Privacy Act 2020 16
Appendix E – Health Information Privacy Code 2020 17
Appendix F – Official Information Act 1982 21
Appendix G – Health Act 1956 22
Appendix H – Health and Disability Commissioner Act 1994 22
Appendix I – Ethics guidelines 22

Introduction

Action for Smokefree 2025 (ASH; ASH NZ) is responsible for data collected to monitor and evaluate ASH's programmes and campaigns, as well as the ASH Year 10 Snapshot Survey. Data is disseminated in many ways, including descriptive reports, fact sheets, data tables, journal articles, and data sets.

ASH data sets are potentially available for statistical purposes to bona fide public good researchers working within academic institutions, government agencies and the wider health sector, subject to certain conditions.

Good statistical practice and our ethical obligations to survey participants require that information collected through ASH surveys, particularly personal information that could be used to identify individuals, is treated as confidential and stored securely. ASH must balance the benefits of data access with its obligations to hold intellectual property and data securely, and protect the confidentiality of information supplied by individuals. Failing to adequately protect individual information potentially reduces public trust and confidence in ASH, and wider government, which in turn affects the ongoing quality of data collections. For more information on relevant legislation, protocol, and guidelines please see Appendix A – Relevant legislation, protocol, and guidelines.

This document outlines ASH's policy for providing access to ASH data and describes the way the policy is implemented. It covers the preparation of data for use, the application and approval process for accessing ASH data, and the monitoring of data set use by researchers.

The ASH NZ Data Access Policy applies to all external researchers who request access to ASH intellectual property (IP) and data.

Data Access Policy

Principles

Principle 1 – Data

1.1 The process for making decisions on access to data will be transparent.
1.2 Any data of suitable quality that is owned (or managed) by ASH is potentially eligible for research use.
1.3 Data sets will be produced in accordance with Principle 4 (Quality) and Principle 5 (Confidentiality).
1.4 Access to data sets is subject to the level of demand, availability of resources and confidentiality risk.
1.5 No ownership of data sets is conferred on researchers.
1.6 Where data sets are no longer considered suitable for research use they may be withdrawn from access and will be disposed of (archived or destroyed) in line with the Public Records Act 2005.

Principle 2 – Purpose

2.1 Research must not be inconsistent with the purposes for which the data was collected.
2.2 Research must be for public good purposes, with clear value and benefits for New Zealand. Access to data is not permitted where people or organisations stand to gain commercially.
2.3 The value of using data rather than other sources of information must be shown.
2.4 Research must be achievable using the data set (i.e., it must be valid and possible), based on scientifically sound methodology, and satisfy any appropriate research ethics requirements.
2.5 Research results must be made publicly available. ASH must be informed prior to the dissemination of results, such as publications and presentations, in order to be aware, in advance, of potential public interest.
2.6 Researchers are expected to commit to undertaking research and disseminating results in a timely manner.

Principle 3 – Researchers

3.1 Researchers proposing research consistent with Principle 2 (Purpose) are eligible to apply for access to data, subject to the following criteria:

- They are connected to a recognised organisation.
- They have a proven history of public good research or are supervised by a person with a proven history of public good research.
- The research team includes a researcher (statistician/analyst) with recognised skills in analysing survey data sets.
- A student is not the lead researcher.

3.2 Access to data is a privilege, not a right. In collecting the data, ASH has an obligation to individuals to protect their information. All researchers must agree to accept these obligations by adhering to

terms and conditions of access. Failure to do so will result in penalties, which may include publication of details relating to any breach and a restriction on access in future.

Principle 4 – Quality

Data sets

4.1 Data sets provided to researchers will be high quality, containing as much detail as possible, notwithstanding the need to safeguard individual information.

4.2 Data sets will be supported by sufficient metadata to allow appropriate research.

Outputs

4.3 Researchers must produce good quality outputs that are subject to acceptable quality assurance processes.

4.4 Researchers must follow any quality rules and statistical obligations stipulated in the metadata, by ASH and/or by the data owner.

Principle 5 – Confidentiality

Data sets

5.1 The confidentiality of individual information will be maintained by modifying data sets to reduce disclosure risk in accordance with ASH disclosure control rules, as outlined:

- All details will be removed that are likely to lead to spontaneous recognition of an individual.
- Data sets will be modified, using standard techniques and processes, so that the identification of individual information is unlikely without a disproportionate amount of time, effort and expertise on behalf of an intruder.
- Researchers must abide by obligations in the Privacy Act.

Outputs

5.2 Researchers must apply any confidentiality rules stipulated in the metadata, by ASH and/or by the data owner, before outputs are released.

5.3 In addition, researchers must ensure that outputs are presented in such a way that individual information is safeguarded should data set modification and confidentiality rules be insufficient protection.

Principle 6 – Security

Despite steps taken to anonymise data, it is important to also protect the security of data sets in the event that the data set modification is insufficient and to prevent public concerns or perceptions about how individual information is being used.

6.1 Researchers will maintain the security of individual information by complying with relevant terms and conditions with regard to access, use, storage and disposal of data sets.

Principle 7 – Review, modification and audit

7.1 This policy will be updated as required to ensure it remains relevant and workable for both ASH and external researchers.

7.2 ASH will periodically undertake an audit of a small number of external research projects.

General terms and conditions

An application to access ASH data assumes that researchers agree to comply with the following general terms and conditions.

1. The organisation responsible for the research team must enter into a *Data License Agreement* with ASH, which sets out specific terms and conditions. The lead researcher must send a copy of the signed *Data License Agreement* to ASH, retain the original on file and make it available for audit, as required.

4. The research team will be responsible for all research undertaken. No support will be provided by ASH staff unless they are formal collaborators on a project, apart from that necessary to ensure that sufficient information is available to allow the proposed research to be undertaken.

5. The data can only be used for the research project described in the *Data License Agreement.*

6. No attempts are to be made to data-match or identify individuals or schools in the data.

7. Security of data sets used off-site:
   - The data and any outputs, which are not sufficiently anonymised, may be accessed only by authorised researchers.
   - Limited copying of the data may be made where reasonably required to permit the research.
   - All researchers are to ensure the safe storage of the data, any part of it, and any printout. Safe storage means the data is protected from accidental or deliberate access by unauthorised people, either physically or electronically, for example, storing the USB drive and printouts in a locked cabinet and password protecting electronic data.
   - At the conclusion of the research, electronic copies of the data sets, any parts, and any insufficiently anonymise outputs must be destroyed. The lead researcher must verify this in writing in their final update. The hard copy USB drive must be returned to ASH.

8. Output confidentiality:
   - Researchers are responsible for output confidentiality.
   - Researchers must apply any confidentiality rules stipulated in the metadata, by ASH NZ and/or the data owner, before outputs are released.
   - Researchers must actively consider whether outputs could be a disclosure risk even with the confidentiality rules applied and take further steps to protect the output if necessary.
   - Outputs cannot be provided to anyone who is not a named researcher with the project unless they have been sufficiently anonymised.

9. Breaches in security or confidentiality:
    - The lead researcher is responsible for immediately advising ASH about any breach of confidentiality or security.
    - Breaches that are deliberate or a result of a lack of due care may result in the termination of access and affect future access requests.

10. Output quality:
    - Researchers are responsible for the quality of all analytical outputs.
    - Researchers must follow any statistical obligations and quality rules stipulated in the metadata, by ASH and/or the data owner.

11. Results of research:
    - The lead researcher must agree to a reasonable timeframe for completing the research and publishing results.
    - All results must include an appropriate reference to the source of the data collection.
    - All results must include a disclaimer indicating that the researchers take full responsibility for the outputs. For example: *The results presented in this paper are the work of the authors.*
    - The lead researcher must send copies of results, publications and presentations to ASH at least one week **prior to dissemination**, so that ASH is informed before any public interest is generated. Failure to do so could affect access to ASH IP or data.
    - ASH may publish links to published work on its website.

12. ASH may request the lead researcher to provide an update of progress, covering what has been achieved, what results have been published, what is planned for the next year, and a list of the current research team.

13. At completion of the research, the lead researcher must return the data, confirm in writing that all confidential material has been destroyed, and provide details of all published or forthcoming results (even where already advised). Researchers are also welcome to provide comments on their experiences with accessing ASH data.

Procedure

How to apply for access

External researchers are required to apply for access to data using the *Data Access Application Form*.

Access to data is subject to the application being approved, a *Data License Agreement* between ASH and the lead researcher's organisation being signed.

It is the lead researcher's responsibility to ensure that the process described below is followed.

1. ASH *Data Access Policy for External Researchers*, which is available on the ASH website. This outlines ASH's Data Access Policy, general terms and conditions for data access, and the process for requesting access to data. An application to access data assumes researchers agree to comply with general terms and conditions for data access.

2. Check the availability and content of the data set(s) of interest. This involves:
   a) Consulting ASH to determine whether a data set is available.
   b) Checking any information provided about the data set (e.g., the questionnaire and/or any methodology reporting) to ensure that the data are available to support the proposed research.

3. Check the fit between the proposed research and the purposes for which the data were collected to ensure that these are not inconsistent (Data Access Policy Principle 2 – Purpose).

4. Check that criteria for researcher access to the data set are met (Data Access Policy Principle 3 – Researchers).

5. Contact the ASH with any queries.

6. Complete a *Data Access Application Form* with supporting material attached, including:
   a) a CV for the lead researcher,
   b) a declaration signed by an authorised delegate of the organisation, who is not one of the researchers, indicating support for the research and confirming that the researchers will abide by the terms and conditions of access,
   c) any other relevant background material.

7. Send the completed application form and supporting material to ASH.

The decision-making process

Upon receiving the application form and supporting material from an external researcher, ASH will undertake the following steps.

1. Acknowledge receipt of the application and advise the applicant approximately how long the decision process is likely to take.

2. The ASH Team will consider the application and provide their recommendation. They will consider whether the application is consistent with the principles in the ASH *Data Access Policy*:
   a) data set availability
   b) compliance with purpose and researcher criteria
   c) likely quality (of outputs)
   d) security or confidentiality concerns.

3. We must balance public interest in the activities of ASH with the obligation to provide data to those who request it. With this in mind, ASH has first priority for using the data. Priority for data access will be given to researchers from organisations who have worked in partnership with ASH in the management or collection of the relevant data. Priority will then be given to researchers who have overseen or contributed to the relevant survey via a Research Coordinating Group, Expert Reference Group or other such group as recognised by ASH. While these priorities need to be considered, our obligation is to provide access to the data, where appropriate.

4. The ASH Director will consider the recommendation and make a decision.

5. ASH will then advise the lead researcher of the outcome.

6. If the application is successful, the lead researcher's organisation must sign a *Data License Agreement* that outlines specific terms and conditions. All members of the research team must sign a *Data License Agreement*.

7. If the application is unsuccessful, the lead researcher may resubmit an amended application or send a submission to the ASH Director for further consideration and review.

Dataset production

If the application is successful, then ASH will follow the below procedure to generate the required dataset(s).

1. As ASH is a small not-for-profit organisation, a minimum charge of NZD95 is applicable to cover costs of producing the dataset(s). More complex applications will incur a higher fee – a quote will be provided before dataset(s) are produced.

2. Data will include no identifying information likely to lead to spontaneous recognition of an individual record.

3. Produce the dataset and associated documentation.
   - Aim to standardise data production as much as possible to reduce the time and resources required to create it and to reduce the risk of different data inadvertently compromising confidentiality protection.

- Produce metadata, including the disclosure control processes (where possible) and potential limitations of the data that are likely to result from the disclosure control process.
- Identify any rules that researchers will be required to apply to ensure the quality and confidentiality of outputs (e.g., minimum cell size, weighted outputs).

References

Ministry of Health (2011). Current Data Access Policy. Retrieved 22 April 2021 from https://www.health.govt.nz/publication/current-data-access-policy

National Ethics Advisory Committee (2019). National Ethical Standards for Health and Disability Research and Quality Improvement. Wellington: Ministry of Health.

Stats NZ (2007). Principles and Protocols for Producers of Tier 1 Statistics. Wellington: Author.

Te Hiringa Hauora/Health Promotion Agency (2021). Data Access Policy for External Researchers. Wellington: Author.

Appendix A – Relevant legislation, protocol, and guidelines

Official statistics are defined in the Statistics Act 1975 as statistics derived by government departments from:

- Statistical surveys
- Administrative and registration records, and other documents from which statistics are, or could be, derived and published.

Several pieces of legislation and other guidelines are relevant to official statistics. Excerpts that are relevant to accessing individual information are discussed here; however, these cannot be relied on without reference to the full documents, which should be consulted as necessary.[1]

Statistics Act 1975

The work of agencies that produce official statistics is guided by the Statistics Act 1975, as well as other legislation. The Statistics Act sets out obligations on Stats NZ to protect the confidentiality of information provided by persons and businesses. While other agencies providing access to their data sets are not subject to this part of the Act, unless it has been collected jointly with Stats NZ, it provides an example of good practice with regard to security and confidentiality of statistical information. Relevant excerpts are included in Appendix B – Statistics Act 1975.

Official Statistics System Principles and Protocols

The OSS Principles and Protocols (Stats NZ 2007) embody key aspects of the Statistics Act as well as the United Nations Fundamental Principles of Official Statistics. The OSS Principles and Protocols apply to Tier 1 statistics, which do not currently include Te Hiringa Hauora surveys. However, agencies are encouraged to use the OSS Principles and Protocols for other official statistics.

The most relevant principle is Principle 7 – Protecting respondents' information, explained in Appendix C – Official Statistics System (OSS) Protocols.

Privacy Act 2020

The Privacy Act 2020 is designed to promote and protect individual privacy. It establishes principles with respect to collection, use and disclosure of information related to individuals. Relevant excerpts from the privacy principles that relate to storage and access to individual information are provided in Appendix D – Privacy Act 2020.

[1] http://www.legislation.govt.nz/all/browse.aspx

While there are exceptions that permit use for statistical or research purposes, it is good practice to adhere to the principles where possible. The rules in the Health Information Privacy Code 2020 modify the principles of the Privacy Act for health information.

Health Information Privacy Code 2020

This code sets out specific rules for agencies in the health sector to better ensure the protection of individual privacy. The code addresses the health information collected, used, held and disclosed by health agencies. It modifies the information privacy principles in the Privacy Act by rules applying to health information and health agencies as in Appendix E – Health Information Privacy Code 2020.

Official Information Act 1982

This Act makes official information more freely available, provides for proper access by each person to official information relating to that person, and protects official information to the extent consistent with the public interest and the preservation of personal privacy. See Appendix F – Official Information Act 1982.

Health Act 1956

There are minimal requirements in the Health Act about access to information. See Appendix G – Health Act 1956.

Health and Disability Commissioner Act 1994

The Code of Rights is a regulation issued under this Act. It sets out 10 rights applicable to all health and disability consumers, including those involved in research. The most relevant aspect for access to information is Right 1 – Right to be treated with respect.

One of its points states that 'Every consumer has the right to have his or her privacy respected'. See Appendix H – Health and Disability Commissioner Act 1994for details.

Ethics Guidelines

Health and disability ethics committees (HDECs) are established in statute, under section 11 of the New Zealand Public Health and Disability Act 2000. A statutory basis gives the committees a clear source of public authority in the exercise of their functions, as well as a clear line of accountability to parliament. A number of guidelines are available to assist their work. Excerpts from the following document is included in Appendix I – Ethics guidelines.

National Ethical Standards for Health and Disability Research and Quality Improvement

The National Ethics Advisory Committee has developed guidelines on conducting observational studies in an ethical manner that are intended to facilitate high-quality studies, protect the interests of participants, and underpin public assurance of good study conduct (National Ethics Advisory Committee 2019).

Public Records Act 2005

The Public Records Act is relevant to long-term retention and disposal of records, not to providing access to active data sets.

Appendix B – Statistics Act 1975

37 Security of information

(1) Information furnished to the Statistician under this Act shall only be used for statistical purposes.

(4) All statistical information published by the Statistician shall be arranged in such a manner as to prevent any particulars published from being identifiable by any person (other than the person by whom those particulars were supplied) as particulars relating to any particular person or undertaking, unless—
(a) That person or the owner of that undertaking has consented to their publication in that manner, or has already permitted their publication in that manner; or
(b) Their publication in that manner could not reasonably have been foreseen by the Statistician or any employee of the Department.

(5) For the purposes of subsection (4) of this section the Statistician shall make such office rules as he considers necessary.

Appendix C – Official Statistics System (OSS) Protocols

http://www.statisphere.govt.nz/about-official-statistics/principles-and-protocols.htm

Principle 7 – Protecting respondents' information

Respondents' rights to privacy and confidentiality are respected and their information is stored securely. Key elements:

- Legislative and ethical obligations governing the collection of data, confidentiality, privacy and release of outputs are rigorously followed.
- Everyone involved in the production of official statistics is made fully aware of their obligations to protect provider confidentiality and of the legal penalties for wrongful disclosure.
- Survey data provided by respondents is only used for statistical purposes.
- Administrative data, whilst primarily collected for operational purposes, can also be used for statistical purposes as well.
- Respondents' privacy concerns are minimised.
- Respondents' confidentiality is always strictly preserved unless they have explicitly agreed to the contrary.
- Secure practices and processes are used in the production of official statistics.
- Unless specific permission provided in legislation allows otherwise, the same confidentiality standards drawn from legislation that produce data will apply to statistics derived from administrative sources

collected specifically for statistical purposes.

Appendix D – Privacy Act 2020

Principle 5 – Storage and security of personal information

An agency that holds personal information shall ensure—

(a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—
  (i) Loss; and
  (ii) Access, use, modification, or disclosure, except with the authority of the agency that holds the information; and
  (iii) Other misuse; and

(b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Principle 6 – Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled,
  (a) to obtain from the agency confirmation of whether or not the agency holds such personal information; and
  (b) to have access to that information.

(2) Where, in accordance with sub clause 6(1) (b) of this principle, an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

(3) The application of this principle is subject to the provisions of Parts 4 and 5 of this Act.

Principle 10 – Limits on use of personal information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds,

(a) that the source of the information is a publicly available publication; or

(b) that the use of the information for that other purpose is authorised by the individual concerned; or

(e) that the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or

(f) that the information,

(i) is used in a form in which the individual concerned is not identified; or
(ii) is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Principle 11 – Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,-

(a) that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) that the source of the information is a publicly available publication; or

(c) that the disclosure is to the individual concerned; or

(d) that the disclosure is authorised by the individual concerned; or

(h) that the information,
(i) is to be used in a form in which the individual concerned is not identified; or
(ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Appendix E – Health Information Privacy Code 2020

Rule 5 – Storage and Security of Health Information

(1) A health agency that holds health information must ensure—
(a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—
(i) loss;
(ii) access, use, modification, or disclosure, except with the authority of the agency; and
(iii) other misuse;
(b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the health agency, including any storing, processing, or destruction of the information, everything reasonably within the power of the health agency is done to prevent unauthorised use or unauthorised disclosure of the information; and
(c) that, where a document containing health information is not to be kept, the document is disposed of in a manner that preserves the privacy of the individual.

(2) This rule applies to health information obtained before or after the commencement of this code.

Rule 6 – Access to Personal Health Information

(1) An individual is entitled to receive from a health agency upon request—
(a) confirmation of whether the health agency holds any health information about them; and

(b) access to their health information.

(2) If an individual concerned is given access to health information, the individual must be advised that, under rule 7, the individual may request the correction of that information.

(3) The application of this rule is subject to—
(a) Part 4 of the Act (which sets out reasons for refusing access to information and procedural provisions relating to access to information); and
(b) clause 6 (which concerns charges).

(4) This rule applies to health information obtained before or after the commencement of this code.

Rule 10 – Limits on Use of Health Information

(1) A health agency that holds health information that was obtained in connection with one purpose may not use the information for any other purpose unless the health agency believes on reasonable grounds,—
(a) that the use of the information for that other purpose is authorised by—
(i) the individual concerned; or
(ii) the individual's representative where the individual is unable to give their authority under this rule; or
(b) that the purpose for which the information is to be used is directly related to the purpose in connection with which the information was obtained; or
(c) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information; or
(d) that the use of the information for that other purpose is necessary to prevent or lessen a serious threat to—
(i) public health or public safety; or
(ii) the life or health of the individual concerned or another individual;
(e) that the information—
(i) is to be used in a form in which the individual concerned is not identified; or
(ii) is to be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(iii) is to be used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(f) that the use of the information for that other purpose is necessary—
(i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or
(ii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation) or
(g) that the use of the information is in accordance with an authorisation granted under section 30 of the Act.

(2) A health agency that holds health information that was obtained from the testing or examination of a blood sample collected in connection with the Newborn Metabolic Screening Programme shall not use that information unless is believes, on reasonable grounds, that the use is in accordance with Schedule 3.

(3) This rule does not apply to health information obtained before 1 July 1993.

Rule 11 – Limits on Disclosure of Health Information

(1) A health agency that holds health information must not disclose the information unless the agency believes, on reasonable grounds,—

(a) that the disclosure is to—

(i) the individual concerned; or

(ii) the individual's representative where the individual is dead or is unable to exercise their rights under these rules; or

(b) that the disclosure is authorised by—

(i) the individual concerned; or

(ii) the individual's representative where the individual is dead or is unable to give their authority under this rule; or

(c) that the disclosure of the information is one of the purposes in connection with which the information was obtained; or

(d) that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information; or

(e) that the information is information in general terms concerning the presence, location, and condition and progress of the patient in a hospital, on the day on which the information is disclosed, and the disclosure is not contrary to the express request of the individual or their representative; or

(f) that the information to be disclosed concerns only the fact of death and the disclosure is by a health practitioner or by a person authorised by a health agency, to a person nominated by the individual concerned, or the individual's representative, partner, spouse, principal caregiver, next of kin, whānau, close relative, or other person whom it is reasonable in the circumstances to inform; or

(g) that the information to be disclosed concerns only the fact that an individual is to be, or has been, released from compulsory status under the Mental Health (Compulsory Assessment and Treatment) Act 1992 and the disclosure is to the individual's principal caregiver.

(2) Compliance with subrule (1)(b) is not necessary if the health agency believes on reasonable grounds, that it is either not desirable or not practicable to obtain authorisation from the individual concerned and—

(a) that the disclosure of the information is directly related to one of the purposes in connection with which the information was obtained; or

(b) that the information is disclosed by a health practitioner to a person nominated by the individual concerned or to the principal caregiver or a near relative of the individual concerned in accordance with recognised professional practice and the disclosure is not contrary to the express request of the individual or their representative; or

(c) that the information—

(i) is to be used in a form in which the individual concerned is not identified; or

(ii) is to be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(iii) is to be used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(d) that the disclosure of the information is necessary to prevent or lessen a serious threat to—

(i) public health or public safety; or

(ii) the life or health of the individual concerned or another individual; or

(e) the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions; or

(f) that the disclosure of the information is essential to facilitate the sale or other disposition of a business as a going concern; or

(g) that the information to be disclosed briefly describes only the nature of injuries of an individual sustained in an accident and that the individual's identity and the disclosure is—
  (i) by a person authorised by the person in charge of a hospital; and
  (ii) to a person authorised by the person in charge of a news entity;
  and for the purpose of publication or broadcast in connection with the news activities of that news entity and the disclosure is not contrary to the express request of the individual concerned or their representative; or

(h) that the disclosure of the information—
  (i) is required for the purpose of identifying whether an individual is suitable to be involved in health education and so that individuals so identified may be able to be contacted to seek their authority in accordance with subrule (1)(b); and
  (ii) is by a person authorised by the health agency to a person authorised by a health training institution; or

(i) that the disclosure of the information—
  (i) is required for the purpose of a professionally recognised accreditation of a health or disability service; or
  (ii) is required for a professionally recognised external quality assurance programme; or
  (iii) is required for risk management assessment and the disclosure is solely to a person engaged by the agency for the purpose of assessing the agency's risk;
  and the information will not be published in a form which could reasonably be expected to identify any individual nor disclosed by the accreditation quality assurance or risk management organisation to third parties except as required by law; or

(j) that non-compliance is necessary—
  (i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution and punishment of offences; or
  (ii) for the conduct of proceedings before any court or tribunal (being proceedings that have commenced or are reasonably in contemplation); or

(k) that the individual concerned is or is likely to become dependent upon a controlled drug, prescription medicine, or restricted medicine and the disclosure is by a health practitioner to a Medical Officer of Health for the purposes of section 20 of the Misuse of Drugs Act 1975 or section 49A of the Medicines Act 1981; or

(l) that the disclosure of the information is in accordance with an authorisation granted under section 30 of the Act

(3) A health agency that holds health information that was obtained from the testing or examination of a blood sample collected in connection with the Newborn Metabolic Screening Programme shall not disclose that information unless it believes, on reasonable grounds, that the disclosure is in accordance with Schedule 3.

(4) Disclosure under subrule (2) is permitted only to the extent necessary for the particular purpose. Health Information Privacy Code 2020 14

(5) Where under section 22F(1) of the Health Act 1956, the individual concerned or a representative of that individual requests the disclosure of health information to that individual or representative, a health agency—
  (a) must treat any request by that individual as if it were a health information privacy request made under rule 6; and
  (b) may refuse to disclose information to the representative if—
    (i) the disclosure of the information would be contrary to the individual's interests; or

(ii) the agency has reasonable grounds for believing that the individual does not or would not wish the information to be disclosed; or
(iii) there would be good grounds for withholding the information under Part 4 of the Act if the request had been made by the individual concerned.

(6) This rule applies to health information about living or deceased persons obtained before or after the commencement of this code.

(7) Despite subrule (6), a health agency is exempted from compliance with this rule in respect of health information about an identifiable deceased person who has been dead for not less than 20 years.

(8) This rule is subject to rule 12.

Rule 12 – Disclosure of health information outside New Zealand

(1) A health agency (A) may disclose health information to a foreign person or entity (B) in reliance on Rule 11(1)(b) or (c) or 11(2)(a), (c), (d), (f), (i) (j) or (l) only if—
(a) the individual concerned or, where the individual is dead or unable to exercise their rights under these rules, that individual's representative authorises the disclosure to B after being expressly informed by A that B may not be required to protect the information in a way that, overall, provides comparable safeguards to those in the Act, as modified by this code; or
(b) B is carrying on business in New Zealand and, in relation to the information, A believes on reasonable grounds that B is subject to the Act, as modified by this code; or
(c) A believes on reasonable grounds that B is subject to privacy laws that, overall, provide comparable safeguards to those in the Act, as modified by this code; or
(d) A believes on reasonable grounds that B is a participant in a prescribed binding scheme; or
(e) A believes on reasonable grounds that B is subject to privacy laws of a prescribed country; or
(f) A otherwise believes on reasonable grounds that B is required to protect the information in a way that, overall, provides comparable safeguards to those in the Act, as modified by this code (for example, pursuant to an agreement entered into between A and B); or
(g) that the disclosure of the information is in accordance with an authorisation granted under section 30 of the Act.

(2) However, subrule (1) does not apply if the health information is to be disclosed to B in reliance on Rule 11(2)(d) or (j) and it is not reasonably practicable in the circumstances for A to comply with the requirements of subrule (1).

(3) In this rule,—
prescribed binding scheme means a binding scheme specified in regulations made under section 213 of the Act
prescribed country means a country specified in regulations made under section 214 of the Act that are made without any qualification or limitation relating to a class of person that includes B, or to a type of information that includes health information.

Appendix F – Official Information Act 1982

4 Purposes

c) To protect official information to the extent consistent with the public interest and the preservation of personal privacy.

5 Principle of availability

The question whether any official information is to be made available, where that question arises under this Act, shall be determined, except where this Act otherwise expressly requires, in accordance with the purposes of this Act and the principle that the information shall be made available unless there is good reason for withholding it.

9 Other reasons for withholding official information

(2) Subject to sections 6,7,10, and 18 of this Act, this section applies if, and only if, the withholding of the information is necessary to—
(a) Protect the privacy of natural persons, including that of deceased natural persons;

Appendix G – Health Act 1956

22H Anonymous health information

Notwithstanding any enactment, rule of law, or other obligation, any person may supply to any other person health information that does not enable the identification of the individual to whom the information relates.

Appendix H – Health and Disability Commissioner Act 1994

The Code of Rights is a regulation issued under the Health and Disability Commissioner Act 1994, section 74. The Code of Rights sets out 10 rights applicable to all health and disability services consumers, including those involved in research. Investigators conducting observational research, audits and other related activities should be familiar with their responsibilities under the Code of Rights, and should consider their study in light of the rights of (proposed) participants. The Code of Rights is available at the Health and Disability Commissioner's website (www.hdc.org.nz).

Note that some provisions give legal effect to ethical standards. For example, the Code of Rights, Right 4(2), states, "Every consumer has the right to have services provided that comply with legal, professional, ethical, and other relevant standards".

Appendix I – Ethics guidelines

New Zealand Public Health and Disability Act 2000

The Minister of Health has established health and disability ethics committees under this legislation. The Ministry of Health is involved with health and disability ethics committees in an administrative capacity. However, it has no input into the decision-making processes of the health and disability ethics committees and does not comment on individual research applications.

Guidelines assist the work of ethics committees as noted below:

National Ethical Standards for Health and Disability Research and Quality Improvement

https://neac.health.govt.nz/system/files/documents/publications/national-ethical-standards-health-disability-research-quality-improvement-2019.docx (National Ethics Advisory Committee 2019)

General considerations for data collection and re-use of existing data

The following standards apply to both new data collection and re-use of existing data.

Māori data

Māori data refers to data produced by Māori or that describes Māori and the environments they have relationships with. Māori data includes but is not limited to:

- data from organisations and businesses
- data about Māori that is used to describe or compare Māori collectives
- data about Te Ao Māori that emerges from research.

12.1 Māori should be involved in decisions about the primary collection, analysis, and interpretation of Māori data in research contexts.

12.2 Decisions about governance and access to data for secondary purposes should be consistent with the Māori Data Sovereignty principles, developed by Te Mana Raraunga. While these principles were developed for Māori data, their application to all health data is recommended, and reflects good practice.

Data identifiability

There are a number of different levels of data identifiability and terms used to describe them.

12.3 Researchers must accurately describe the identifiability of data to obtain meaningful informed consent and to determine the ethical risk of their studies.

Data from which it can reasonably be assumed that it is possible to identify a specific individual involved in the study through direct identifiers (NHI, name, street address, phone number, online identity, identification numbers) and indirect identifiers (date of birth, identification of relatives, identification of employers, clinical notes, any other direct or indirect identifiers that carry significant risk of re-identification).

Benefits and harms from data use

Health data can generate benefits for individuals and the public both now and in the future. In some cases, it may be unethical not to use data because it may deny these benefits, and a failure to use it may also cause

harm. Researchers must identify the possible benefits and risks of harm of data use, carefully balance them against each other, and consider how to minimise and mitigate any harms of data use.
The nature, degree, and likelihood of benefits resulting from studies is dependent on context, which researchers must consider every time they propose to use health data.

The nature, degree, and likelihood of possible harms resulting from studies also depends on context, which researchers must also consider every time they propose to use health data.

Privacy and confidentiality

The principles of privacy and confidentiality apply to all health data at all points of the data lifecycle.[6]

12.8 Researchers must record and respect restrictions that participants and/or individuals place on the use of their health data.

12.9 Researchers must protect participants' and/or individuals' health data and must only use and disclose it to people authorised by those participants and/or individuals, unless:

- disclosure of the data is required by law
- the researchers believe, on reasonable grounds, there is a serious and imminent threat to public health, public safety or the life or health of an individual.

12.10 Unauthorised disclosure plans should be in place that are compliant with HISO 10064:2017 Health Information Governance Guidelines and the Privacy Act, and adherent to organisational policies and procedures. This plan should include steps to reduce accidental disclosure and data breach, how to inform participants and/or individuals, as well as mitigation steps to limit the impact of accidental disclosure and data breach.

Storage, governance and management of data

Data can be stored in analogue or digital form. Regardless of the form of storage, health data storage must meet the following standards:

12.11 Health data should be stored in a secure manner. Examples of secure storage include: locked file cabinets in locked rooms; password protected databases located on computers in locked rooms; password protected databases via password protected computers; etc.

12.12 Researchers should weigh the benefits and risks of keeping identifiers on stored data.

- some cases, there will be good reasons to maintain an identifier, or a link to an identifier (e.g. to maintain participant and/or individual safety, or to re-use the data).

12.13 Data should not be stored longer than is required for the purposes for which the information may lawfully be used, but should be stored for the minimum period required by New Zealand law (currently 10 years for health data that relates to an identifiable individual).

Robust policies, processes, and procedures must be in place to manage data throughout its life cycle. This requires high-quality, transparent data governance and data management. Appropriate governance and management are especially important in cases where the consent requirement for data use has been waived, where there is data linking, or where unspecified future use is intended. Māori control of Māori data is the primary goal for Māori data sovereignty by improving Māori/iwi access to data for governance decision-making and ensuring Māori/iwi involvement in governance of data.

Data can be primarily collected by a researcher, but in the modern healthcare environment organisations are often the primary data source. This creates a tiered structure of overlapping responsibilities of data guardianship between, on the one hand, organisations that create, store, and allow access to data and, on the other hand, individual researchers who use this data, who may work within or outside the data source organisation.

Data-linking

Data-linking is a technique for connecting pieces of information that are thought to relate to the same person, family, place or event. If these different pieces of information can be connected to a person in a way that does not breach their privacy or cause harm, linking them can create a rich resource for research to answer complex questions and improve health outcomes (Data Linkage Western Australia 2019).

When data sets are linked, the risks of identification and adverse public reaction are likely to be greater, especially when the different data sources (which may apply to individual people, households or organisations), may have been designed and collected without the intention of using them together. The process may give rise to concerns that the combined format produces a detailed picture of individuals that they did not consent to when they supplied the data. Privacy is a major consideration in data linkage work.

12.31 Researchers involved in data-linking must weigh the potential benefits of their research against the risk that individuals will be identifiable within their results. See 'Benefits and harms from data use' and 'Research benefits and harms'.

12.32 Researchers must either seek consent from participants and/or individuals or obtain a waiver from a local data governance committee or an ethics committee for research that involves data-linking with identifiable and re-identifiable data.

12.33 Consent from participants and/or individuals or a waiver from an ethics committee is not required for use of linked non-identifiable data, but researchers should be aware of the type and size of data sets being linked, and how these factors increase the risk of identification.

- Data linked by a third party at the request of a researcher, but provided in a non-identifiable format, is a way of controlling risk of re-identification in research involving linkage.
- Use of linked data that has been rendered non-identifiable presents lower risks than linked identifiable or re-identifiable data; however, risks in relation to interpretation harms and re-identification remain, and researchers must consider them.

12.34 Researchers must respect any conditions concerning data-linking expressed within participants and/or individuals' existing consent. In the absence of direct participant and/or individual consent, a waiver must be sought from an ethics committee.

12.35 The amount of data that is linked should be fit-for-purpose. Researchers must be able to justify re-use of requested data.

12.36 Researchers should be aware that if their research includes data linkage the methods by which that data was collected may result in systematic biases. This in turn may have implications for the validity of the research results.

- Researchers should consider these limitations when designing their research and mitigate the impacts of these biases where possible. They should also be recognised when reporting research results.

12.37 Researchers should account for the destruction of any linked data. If an explicit destruction plan is not specified, then the rationale for archiving should be provided. Any long-term data storage must adhere to local data governance, national standards, and law as applicable.

- In considering how long to hold linked data, researchers must undertake a balancing exercise between the advantages of the robustness of data linkage and the ability to validate data linkage and protection of privacy, and benefits of re-use of data.
- Researchers should be prepared to provide local data governance committees (for example, a research office at a DHB) or ethics committees with a detailed plan of linked data storage, an accounting of the risks of storage, and plans to mitigate the risk of storage.

12.38 Researchers must work within established organisational governance structures, as well as develop specific data management plans that ensure the data is being accessed and linked in an appropriate and responsible manner.

12.39 Researchers must address the privacy risks of linking data by analysing the primary and secondary uses of the data, considering not just re-identification risks but also inference risks.

- Analysis should take into account not only whether a person can be directly associated with a particular attribute, but also the extent to which attributes that may be revealed or inferred depend on an individual's data and the potential harm that may result. In addition, it should take into account the potential uses and analysis of the data, which in turn affect data governance and management.