

6 June 2023

s 9(2)(a)

Official information request HN200017780

I refer to your official information request dated 28 April 2023 regarding Privacy Policy for lab tests. Specifically:

Can you provide us with your Privacy Policy in regards to lab tests and other information collected? The information presented on your website is non.

Please provide the following

- 1. What information is being collected?*
- 2. Who can access this information?*
- 3. Which external organizations do you give our personal data to and what data?*
- 4. The agency that will hold our information?*

Response

LabPlus | Auckland | Te Toka Tumai Auckland | Te Whatu Ora is governed by the local Privacy Policy (enclosed for your information), the Privacy Act and the Health Information Privacy Principles.

Please see:

<https://www.privacy.org.nz/privacy-act-2020/privacy-principles/>
<https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/hipc2020/>

1) What information is being collected?

LabPlus collects the patient's National Health Index (NHI) number, date of birth and name.

2) Who can access this information?

The only people who can access this information are laboratory staff, who all sign confidentiality agreements as a condition of their employment with Te Toka Tumai Auckland. Laboratory staff are only authorised to access samples they are specifically delegated responsibility for.

We are not able to list the number of agencies who would have access to your data as any agency who are providing you care may have access. A good source for the names of those external organisations is Health Navigator: <https://www.healthnavigator.org.nz/services-and-support/>

3) Which external organizations do you give our personal data to and what data?

To provide accurate and timely lab test results to support care delivery, we need to collect and use your health information. We make sure that your information is only used and shared by health professionals who need access to it. Sharing health information is important for healthcare providers to provide safe care.

We may share health information about you to:

- GP practices
- Medical Specialists and Consultants involved in the care of specific patients
- Other laboratories, both public and private, who provide services with us
- The healthcare provider who requested your lab tests
- Other healthcare providers with a role in your care, either on request from the provider or by uploading your results to shared clinical databases, including [TestSafe](#) and [Eclair](#)
- Other lab testing facilities, including overseas, where necessary to obtain tests that are not available at our labs
- Your representative, or family/whanau where you have authorised this
- We also share anonymised data for research and statistical purposes.

4) The agency that will hold our information?

We have provided you with our District Privacy Policy. Specifically about laboratories, we can provide the following answers.

We may collect, hold, generate or provide to external agencies the following health information about you:

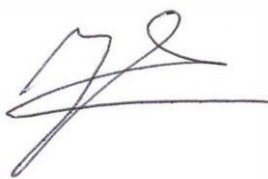
- Name
- Date of birth
- Gender
- Ethnicity
- Occupation
- Address (postal and email)
- Telephone numbers
- Emergency contact information
- NHI number
- Medical history provided by the referrer
- Previous test results
- Information who referred you for a test
- Test results prepared in relation to your current request

If you have any questions, you can contact us at hnzOIA@health.govt.nz.

If you are not happy with this response, you have the right to make a complaint to the Ombudsman. Information about how to do this is available at www.ombudsman.parliament.nz or by phoning 0800 802 602.

As this information may be of interest to other members of the public, Te Whatu Ora may proactively release a copy of this response on our website. All requester data, including your name and contact details, will be removed prior to release. The released response will be made available on our website.

Nāku iti noa, nā

A handwritten signature in black ink, appearing to be 'MS', written over a light blue grid background.

Dr Mike Shepherd
Interim District Director
Te Toka Tumai Auckland

Enclosure - Te Toka Tumai Auckland Privacy Policy

Privacy Policy

Unique Identifier	PP01/I&R/009 - v01.00
Document Type	Policy
Risk of non-compliance	may result in significant harm to the patient/DHB
Function	Administration, Management and Governance
User Group(s)	Auckland DHB only
<ul style="list-style-type: none"> • Organisation(s) • Directorate(s) • Department(s) • Used for which patients? • Used by which staff? • Excluded 	Auckland District Health Board All directorates All departments All patients All staff
Keywords	
Author	Adapted from National DHB Privacy document
Authorisation	
<ul style="list-style-type: none"> • Owner • Delegate / Issuer 	Chief Health Professions Officer & Privacy Officer Director - Information Management Operations
Edited by	Document Control
First issued	11 May 2021
This version issued	11 May 2021 - issued
Review frequency	3 yearly

Contents

1. Purpose of policy	3
2. Policy statements.....	3
2.1 Guiding values	3
2.2 Scope	3
2.3 Data protection and use policy	4
3. Definitions.....	4
4. Privacy Act 2020 and Health Information Privacy Code 2020.....	6
4.1 Collection.....	7
4.2 Security.....	8
4.3 Access, correction and accuracy	9
4.4 Retention.....	10
4.5 Use and disclosure.....	11
4.6 Unique identifiers.....	14
5. Privacy breaches/ Interference with privacy.....	14
5.1 Managing a privacy breach	14
5.2 Interference with privacy	15
5.3 Lodging a complaint	15
6. Compliance, offences and fines.....	15
7. Privacy impact assessments/ Privacy by design	17
7.1 Completing a Privacy Impact Assessment (PIA)	17
7.2 Privacy by design	17

8. Research, audit, quality assurance and quality improvement	17
9. Support and administration.....	18
9.1 Roles and responsibilities	18
9.2 Training.....	18
9.3 Queries and complaints.....	18
10. Supporting evidence	18
11. Legislation	18
12. Associated documents.....	19
13. Disclaimer	19
14. Corrections and amendments	19
Appendix 1: Detailed roles and responsibilities.....	20

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

1. Purpose of policy

The purpose of this policy is to:

- Provide guidance and confirm Auckland DHBs expectations about the management of personal and health information, including the collection, storage, use, retention and destruction of that information.
- Outline our requirements to comply with the Information Privacy Principles and Health Information Privacy Rules under the Privacy Act 2020 and Health Information Privacy Code 2020.
- Support DHB personnel in dealing with complaints and potential breaches of privacy

2. Policy statements

2.1 Guiding values

The following guiding values support this policy:

- Privacy is about managing and protecting personal and health information about an **individual**. We are mindful of the trust relationship and respectful of our obligations as kaitiaki¹ and guardians of information we hold about individuals.
- Privacy is everyone's responsibility.
- When dealing with personal and health information it should be treated with the same care and respect as if it were our own.
- We have a transparent and open approach to managing personal and health information.
- We build privacy into the design and implementation of our facilities, services, processes and systems.
- We know, promote and comply with our legal, ethical and individual professional obligations.
- We acknowledge and incorporate the New Zealand Governments Social Investment Agency (2019), Data Protection and Use Policy values of *He tāngata; Manaakitanga; Mana whakahaere; Kaitiakitanga; and Mahitahitanga* into all privacy practices (see [Supporting evidence](#)).

2.2 Scope

This policy applies to all DHB personnel handling personal and health information. DHB personnel must:

- Observe the legal requirements that govern the collection, security, access, retention, use and disclosure of personal and health information.
- Familiarise themselves with this policy, the associated procedures, the Privacy Act 2020, the Health Information Privacy Code 2020, privacy/confidentiality obligations in their employment/contractor agreements and policy by their professional registration body appropriate to their role.
- Read this policy alongside the associated procedures to support informed and good decision making.

¹ (noun) trustee, minder, guard, custodian, guardian, caregiver, keeper, steward.

2.3 Data protection and use policy

This policy includes considerations from the Data Protection and Use Policy (DPUP). DPUP recommends good practice above and beyond the minimum legal requirements of the Privacy Act 2020. DHBs are not legally bound by DPUP but are encouraged to consider it when collecting, using and sharing information.

DPUP consists of five Principles²:

- **He tāngata**- Focus on improving people's lives — individuals, children and young people, whānau, iwi, and communities
- **Manaakitanga** - Respect and uphold the mana and dignity of the people, whānau, communities or groups who share their data and information.
- **Mana whakahaere** - Empower people by giving them choice and enabling their access to, and use of, their data and information.
- **Kaitiakitanga** - Act as a steward in a way that is understood and trusted by New Zealanders.
- **Mahitahitanga** - Work as equals to create and share valuable knowledge.

DPUP has a collectively developed Toolkit containing more information for implementing DPUP available on their website (see <https://dpup.swa.govt.nz/>).

3. Definitions

The table below sets out an agreed definition for terms in this policy and associated procedures:

Term	Definition
Data Protection and Use Policy	The 'Data Protection and Use Policy', articulates what 'doing the right thing' looks like across the social sector in its collection and use of people's data and information. What personal data and information people share, who they share it with and how they share it matters. Building and maintaining trust is key. The policy comprises five principles, which articulate the values and behaviours that underpin the respectful and transparent use of data across the social sector. DPUP was developed by the social sector, for the social sector, after extensive and inclusive engagement with agencies, iwi and communities. For further information see the Social Wellbeing Agency's website (see https://dpup.swa.govt.nz/).
DHB personnel	'DHB personnel' means a person who carries out work for a district health board, including work as an employee, board member, contractor, subcontractor, employee of a contractor or subcontractor, an employee of a recruitment company who is assigned to work at a DHB, a trainee or student, a person gaining work experience or undertaking a work trial or a volunteer.

² Built upon, but separate to the Information Privacy Principles in the Privacy Act 2020

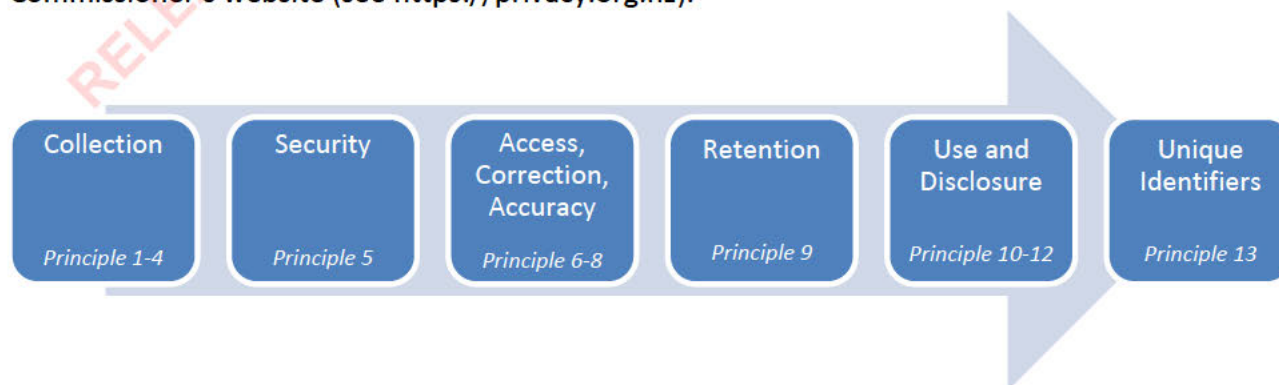
Term	Definition
Health information	'Health information' means information about an identifiable individual's health. This includes information about their health or disabilities, their medical history, health or disability services provided to them, information about donating organs or blood and information collected while providing health and disability services, such as addresses for billing purposes or information relevant to funding. Examples of health information are: clinical notes, genetic information, test results, diagnostic images, verbal discussion and records of conversations. This includes information about both a living individual and a deceased individual.
Individual	An 'individual' means a natural person, such as DHB personnel, a patient or a visitor.
Interference with privacy	An 'interference with privacy' is an action that breaches an information privacy principle under the Privacy Act 2020 and harms or may harm an individual. The legislative definition is here (see https://www.legislation.govt.nz / Privacy Act 2020 / search with in the interference).
Patient	'Patient' or 'service user' means a person receiving health and disability services.
Personal information	'Personal information' means information about a living identifiable individual. This information can be in any form, including paper and electronic documents and files, emails, personnel records and patient records, and can include images such as photos, an image of a pathology report or a diagnostic image. It can also include video recordings, audio recordings. Examples of personal information include an individual's name, telephone number, address (email and postal), date of birth, ethnic origin, tax file number and Health Information. Even if an individual's name does not appear, but there is a reasonable chance that an individual could be identified from the information (including where information can be combined with other information to identify a person), it can still be personal information for the purposes of the Privacy Act.
Privacy breach	A 'privacy breach' occurs when the DHB does not comply with one or more of the Information Privacy Principles set out in Part 3 of the Privacy Act 2020 or rules as defined within the Health Information Privacy Code 2020. Examples include instances where personal information held by the DHB is accessed, disclosed, altered, lost or destroyed without authorisation or by accident or when requests for access to personal information are not processed in a timely manner. A privacy breach may also be something that prevents the DHB from accessing the information on a temporary or permanent basis.
Privacy by design	'Privacy by design' is an approach taken when creating new technologies and systems. It is when privacy is incorporated into

Term	Definition
	tech and systems, by default . It means your product is designed with privacy as a priority, along with whatever other purposes the system serves. The seven principles of Privacy by Design are explained here (see https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/manage-a-privacy-programme/privacy-by-design-pbd/)
Research	Research is any social science; kaupapa Māori methodology; or biomedical, behavioural or epidemiological activity that involves systematically collecting or analysing data to generate new knowledge, in which a human being is exposed to manipulation, intervention, observation or other interaction with researchers either directly or by changing their environment, or that involves collecting, preparing or using biological material or medical or other data to generate new knowledge about health and disability.
Third Party (includes other agencies)	'Third Party' or 'Third Parties' means a person or group external to a particular DHB. A Third Party could be a healthcare provider (such as a primary health organisation or another DHB), a government agency (such as Police, Oranga Tamariki), or other individuals (such as whanau or family of a patient).

4. Privacy Act 2020 and Health Information Privacy Code 2020

The Privacy Act 2020 sets out 13 information privacy principles to govern the collection, security, access, retention, use and disclosure of personal information. The Health Information Privacy Code 2020³ is a code of practice under the Privacy Act 2020 to govern health information. The 13 rules of the Health Information Privacy Code 2020 complement the 13 information privacy principles of the Privacy Act 2020.

The 13 information privacy principles from the Privacy Act 2020 and rules from the Health Information Privacy Code 2020 are summarised in the following section of this policy, as shown in the diagram below. To see the rules and principles in full please refer to the Office of the Privacy Commissioner’s website (see <https://privacy.org.nz>).



³ See <https://privacy.org.nz/privacy-act-2020/codes-of-practice/hipc2020/>

4.1 Collection

Expected values and behaviours

He tāngata

Focus on improving New Zealanders' lives — individuals, children and young people, whānau, iwi, and communities.

- Strive to create positive outcomes from any collection, sharing or use of data and information.
- Use appropriate checks and balances and ensure that information is suitable and reasonably necessary for the intended outcome.

Manaakitanga

Respect and uphold the mana and dignity of the people, whānau, communities or groups who share their data and information.

- Recognise and incorporate diverse cultural interests, worldviews, perspectives and needs.
- Include and involve service users whenever possible.
- Incorporate the needs and priorities of people with a specific or particular interest in what is done with their data and information.

Only collect personal and health information if you really need it – [Principle 1/ Rule 1]

Information must only be collected if it is necessary for purposes connected with the DHB's functions. Patient health information may be collected to provide care and treatment, administration, training and education and monitoring quality of care. Personal information relating to DHB personnel may be collected for purposes including determining job suitability, work performance, workplace health, safety and security of DHB assets, workforce planning and administration.

Collect only the information required to fulfil your objectives; this can include questions you ask of patients, but also software settings for equipment you use.

Consider DPUP value '**He tāngata**': Are the purposes of collection clearly focused on positive outcomes and is the information to be collected necessary to achieve those outcomes? Purpose will always be relevant. Assessing and articulating it properly is vital to both legal compliance and guarding against indiscriminate or excessive collection of people's information.

Get it straight from the individual concerned – [Principle 2/ Rule 2]

Information should be collected from the individual who is the subject of the information. If you want information about an individual, just ask them.

Consider DPUP value '**Manaakitanga**': Complete forms, assessments or records together with patients or relevant individuals.

In some situations, information can be collected from other people such as next of kin or who have the individual's consent or authority to act on their behalf.

Tell the individual what you will do with their information – [Principle 3/ Rule 3]

When you collect information, let the individual know why it is being collected, who will receive it, whether collecting it is voluntary and what will happen if it is not collected. An explanation is not necessary if doing so is impractical, against the individual's interests or prejudices the purpose of collection.

This explanation could be a privacy statement on a form, a wall poster, patient information brochure, statement on DHB website or discussed in conversation. ADHB includes this explanation in its patient registration form.

Consider DPUP value '**kaitiakitanga**': As kaitiaki or stewards of individual's personal information, can the purposes of collecting be easily explained to individuals and in a way that fosters understanding and trust in what is being done with their information?

Be considerate when you collect the information – [Principle 4/ Rule 4]

Collect information in a way that is lawful, fair, open and transparent. Information cannot be collected by unlawful, unfair or intrusive methods. This is particularly important when collecting information from a child, young person or vulnerable adult – take extra care.

Some examples:

Collection is unlawful if it is in breach of another law. Collection is unfair if it is done in a threatening or misleading way. Collection is unreasonably intrusive if you collect information without respecting cultural needs or the individual's preferences.

4.2 Security

Expected values and behaviours

Kaitiakitanga

Act as a steward in a way that is understood and trusted by New Zealanders.

- Recognise you are a kaitiaki, rather than an owner of data and information.
- Be open and transparent; support people's interest or need to understand.
- Keep data and information safe and secure and respect its value.

Take care of it once you have got it – [Principle 5/ Rule 5]

Take reasonable steps to ensure that all information collected about an individual is protected against loss, unauthorised access, misuse, modification or disclosure. Consider kaitiakitanga: keep information safe and secure and respect its value.

Note: For specific guidance regarding security measures required to protect patient and other personal or business related information at Auckland DHBs Information Security policy (see [Associated documents](#)).

Some examples:

Auditing is useful way to pick up a common misuse: unauthorised browsing by DHB personnel. A Privacy Impact Assessment provides assurance that appropriate privacy risks have been considered to support security and data governance.

Consider DPUP value '**kaitiakitanga**': Understand that as a steward of the data, we must keep data and information safe and secure and respect its value:

- Use data management practices that are safe and secure, bearing in mind the nature of the information and data, and how it is being collected, used, shared, analysed and reported.
- Treat data as a valuable asset. Store and maintain it so that it is accessible and reliable.
- Those who hold people's information are in a position to grow its value. They may do this by creating and sharing insights, or by returning collective, non-personal data back to the people and community it came from for their use. In all cases they must take care to comply with the law, protect people's privacy and maintain people's trust and confidence.

4.3 Access, correction and accuracy

Expected values and behaviours

Mana whakahaere

Empower people by giving them choice and enabling their access to, and use of, their data and information.

- Where possible, give people choices and respect the choices they make.
- Give people easy access to and oversight of their information wherever possible.

Access and correction requests must be dealt with in accordance with the Clinical Records Management policy. Requests for access or correction of personal and health information can be made verbally or in writing, and should be directed to Auckland DHB Clinical Records Department.

When dealing with access and correction requests the Clinical Records team may contact the relevant clinical service and/or the Auckland DHB Legal team for input and assistance.

An individual can see their personal and health information if they want to – [Principle 6/ Rule 6]

Everyone has the right to access information about themselves. However, a DHB may refuse access to the information if there are good reasons. This principle is about access to information, and not ownership of information. You must take care that the person who is requesting the information is that person or their approved representative. Please note that it is an individual's **legal right** to make a request to a DHB to confirm if the DHB holds any personal information about them, and to have access to that information.

Consider DPUP value '**mana whakahaere**': Consider the following:

- Give people easy access to and oversight of their information wherever possible
- Encouraging people to see what is recorded about them is a way of empowering them and acknowledging that their data and information is part of their story and experiences.
- Making it easy for people to see their data and information can mean many things — from showing them what is written on a computer screen, to including them on email referrals to another agency (taking care to double-check email addresses), to providing information in accessible formats for people with a sight disability or limited literacy. The important thing is that people shouldn't have to rely on Privacy Act requests to access information held about them.
- Whenever possible, help people check, add, or correct their information.
- Help people access their information so that they can share it with others and avoid retelling their story if that is what they want.

Some examples:

An individual's access to information can be declined if allowing access to the information would pose a serious threat to life, health or safety, or lead to serious harassment. A complete list of reasons to refuse access is set out in sections 49-53⁴ of the Privacy Act 2020.

The Office of the Privacy Commissioner may direct a DHB to provide an individual access to their personal and health information if the DHB refuses access without a proper basis. See [Section: 6 Compliance, offences and fines](#).

An individual can ask to correct their information if they think it is wrong – [Principle 7/ Rule 7]

Everyone has the right to request a DHB to correct the information held about them. Correction may involve amending, deleting or adding information, if the request is reasonable and necessary to ensure accuracy.

A DHB must give reasonable assistance to the individual who wishes to make a correction and may have to transfer the request to another DHB if necessary. If a DHB does not believe the information needs correcting, it must take reasonable steps to attach a statement of the correction sought by the individual. You must tell the individual what you have corrected; if you are not going to correct the information, you must tell them what steps you have taken for their request for correction to be added to their records and files.

For further guidance refer to Auckland DHB's Privacy Officer, [Sue Waters](#), for support.

Check the accuracy of information before using it – [Principle 8/ Rule 8]

Ensure the personal and health information is accurate, up to date, complete, relevant and not misleading before you use or disclose it.

4.4 Retention

Get rid of the information once you are done with it – [Principle 9/ Rule 9]

⁴ <https://www.legislation.govt.nz/act/public/2020/0031/latest/whole.html#LMS23392>

Personal and health information should only be kept for as long as it is required for the purpose it was collected. Health information must be retained under certain legislation, and this overrides the Health Information Privacy Code 2020 and the Privacy Act 2020, to the extent that they are inconsistent.

Some examples:

- *Health (Retention of Health Information) Regulations 1996* require all health information to be retained for ten years from the last encounter with the patient, unless transferred to another doctor or to the patient.
- *The Public Records Act 2005* also mandates retention of records. The DHB General Disposal Authority lists how long each type of clinical record must be kept for and what must be done with it afterwards.

Once the obligatory retention periods have passed, personal information should be disposed of, securely, unless there is a lawful purpose to retain it.

Sometimes health and personal information may need to be kept longer for special reasons.

Example:

DHBs must currently hold some information indefinitely due to the Royal Commission of harm while in State Care (see <https://archives.govt.nz/publications/disposal-moratorium-royal-commission>).

Refer: Auckland DHB's Corporate Records site on HIPPO to learn about the storage of records (see <https://adhb.hanz.health.nz/Pages/Corporate-Records.aspx>).

4.5 Use and disclosure

Expected values and behaviours

He tāngata

Focus on improving New Zealanders' lives — individuals, children and young people, whānau, iwi, and communities.

- Strive to create positive outcomes from any collection, sharing or use of data and information.

Mahitahitanga

Work as equals to create and share valuable knowledge.

- Work with others across the sector to create and share value together.
- Confidentially share relevant information between professionals so people get the support they want and need.
- Make sure there is a two-way street of sharing (de-identified) data, analysis, results and research findings to grow collective knowledge and improve services.

Use it for the purpose you got it – [Principle 10/ Rule 10]

Personal and health information should generally be used for the same purpose for which it was collected. Consider the purposes for which information is being collected at the time of collection

(see Principle 1 / Rule 1 above). Principle 10 / Rule 10 permit a DHB to use the information for those legitimate purposes connected with the DHB's functions.

A new use of information is allowed in certain situations.

Only disclose the information if there is a good reason – [Principle 11/ Rule 11]

Disclosure is permitted if the individual consents or disclosure is one of the purposes for which the information was collected. Information must be disclosed if another law requires it. Information can also be disclosed in certain situations if it is not appropriate to obtain the individual's consent. Only disclose the information required to fulfil the requirement and try to avoid excessive sharing.

There are several situations where a DHB is permitted to disclose information under rule 11. This policy does not describe all those situations. However, DHBs most frequently disclose information in the following situations:

- Disclosure is authorised by the individual or their representative
- Disclosure was one of the purposes for which the DHB got the information, e.g. sharing the hospital discharge notes with the patient's General Practitioner
- Disclosure is necessary to prevent a serious threat to an individual's life or safety
- Disclosure is necessary for court proceedings or to maintain the law
- Disclosure is for statistical / research purposes.

Information must be disclosed if it is required by a compulsory legal authority that overrides the Privacy Act 2020, such as:

- a production order or search warrant by New Zealand Police
- a request for information about child care and protection under section 66 of the Oranga Tamariki Act 1989 by police or Oranga Tamariki
- a request for health information, requested by any person providing health services to the individual under section 22F of the Health Act 1956.

Information can be disclosed in certain situations if it is not appropriate to obtain the individual's consent, such as:

- Information may be disclosed if necessary to prevent a serious threat to any individual's life or safety, or to avoid prejudice to the maintenance of the law or for statistical/research purposes, under information privacy principle 11;
- Health information may be disclosed, on request, to New Zealand Police, Oranga Tamariki or a probation officer under section 22C of the Health Act 1956
- Information may be disclosed via a report of concern to Oranga Tamariki if a child is at risk, under section 15 of the Oranga Tamariki Act 1989
- Information may be proactively shared with specified agencies and persons for the well-being or safety of a child and / or to respond to family violence.

Consider DPUP value '**Mahitahitanga**': Confidentially share relevant information between professionals so people get the support they want and need.

- Recognise the diverse and complex nature of the sector and use it as an opportunity. In many situations, no single professional or agency will have the whole picture.
- Enable other professionals to support service users by making sure they have the information they need to do their work, within what the law permits.

Make sure there is a two-way street of sharing (de-identified) data, analysis, results and research findings to grow collective knowledge and improve services.

- Enable organisations/groups with a clear and legitimate interest to safely and easily access and use government held data sets in a de-identified form, for locally led development.
- Share expertise and help others understand and use data accurately and safely, for example, ensuring it is not re-identified.
- Advocate for, and support 'by/for' research, like Kaupapa Māori, so communities or groups better understand their own goals and priorities and the needs of their people.
- Create feedback loops with people and organisations who contribute data and information. Tell them the outcomes of any use and the value it created.

Only disclose information overseas if it is safe to do so for the individual – [Principle 12/ Rule 12]

Information may only be disclosed overseas if the overseas recipient (a foreign person or entity):

- Is subject to the Privacy Act 2020 because they do business in New Zealand;
- Is subject to privacy laws that provide comparable safeguards to the Privacy Act 2020;
- agrees to protect the information in a way that provides comparable safeguards to the Privacy Act 2020, e.g. contractual clauses between the parties provide for privacy obligations; and/or
- Is covered by a binding scheme or is a country prescribed by the New Zealand government.

If the overseas recipient does not meet one of the above requirements, then seek authorisation from the individual. The individual must be expressly informed that the overseas recipient organisation may not be required to protect the information in a way that provides comparable safeguards to the Privacy Act 2020. If the individual does not provide authorisation, then do not disclose the information overseas. Talk to the Privacy Officer and/or Legal Services to explore other options.

Take care to note that these obligations do not apply if the information is urgently required overseas to maintain the law or to prevent or lessen a serious threat to public health, safety, or an individual's life or health (both for the individual concerned, and also for another individual whose life or health is under serious threat as the case may be).

Sending information to an overseas cloud storage service to hold information on the DHB's behalf is not considered to be an overseas disclosure of information, as the storage service is holding the information on behalf of the DHB for safe custody under section 11 of the Privacy Act 2020.

The Privacy Act 2020 has extraterritorial effect; this means it applies to overseas agencies in relation to actions taken by them while carrying on business in New Zealand. Therefore if you are sending information to a foreign entity (for the purposes of IPP 12) who is also an overseas agency (for the purposes of section 4), they will be subject to the Privacy Act in respect of the personal

information that they hold in the course of carrying on business in New Zealand, and this gives you a basis to disclose information overseas.

In short, when sharing information to a foreign person, authority or country, an individual's privacy should be protected the same if not better than if it was shared in New Zealand.

4.6 Unique identifiers

Only use unique identifiers where necessary – [Principle 13/ Rule 13]

National Health Index (NHI) numbers are assigned and used to identify patients, instead of using their names. Unique identifiers are also assigned to DHB personnel to support the identification of the individual. Unique identifiers are used to support patient care and DHB personnel management only – they must not be used or shared for other reasons.

Unique identifiers should only be used in the context they are created; if it is not necessary to use a unique identifier like an NHI number and you can use a patient's name, you can avoid using the NHI number. For instance when sending a letter addressed to the patient, consider if it is necessary to include a unique identifier when the patient's name will do.

5. Privacy breaches/ Interference with privacy

5.1 Managing a privacy breach

If DHB personnel suspect or are aware that there has been a possible privacy breach or near-miss, they must immediately activate the Auckland DHB Privacy Breach Guideline (see [Associated documents](#)).

It is important to respond to a suspected or actual privacy breach as quickly as possible so that the DHB can deal with it immediately and minimise the harm to the affected individuals. Being transparent, clear and open with the impacted individuals is critical to maintaining their trust. Full reporting of all incidents provides the DHB with an opportunity to improve processes or systems to avoid future breaches. Under the notifiable privacy breach framework, a DHB is required to notify the Office of the Privacy Commissioner and the affected individual if the breach caused 'serious harm' to the individual.

Important: See the Auckland DHB Privacy Breach Response Procedure which details the roles and responsibilities for investigating, assessment and reporting through to the Office of the Privacy Commissioner for breaches that meet the 'serious harm' threshold.

Key steps in managing a breach:

- Contain the breach and make a first assessment (Use the Office of the Privacy Commissioner's Notify Us Tool – see <https://privacy.org.nz/responsibilities/privacy-breaches/notify-us/evaluate>)
- Evaluate the breach
- Notify affected people if necessary
- Prevent the breach from happening again

The DHB Privacy Officer will confirm whether there has been a notifiable privacy breach that triggers notification to the Office of the Privacy Commissioner and the affected individual/s. Failure to notify the Office of the Privacy Commissioner of a notifiable privacy breach is an offence and can result in a fine up to \$10,000.

Note: Further guidance can be found in the Auckland DHB Privacy Breach Guideline (see [Associated documents](#)).

5.2 Interference with privacy

An interference with privacy is caused when the DHB breaches one of the privacy principles of the Privacy Act and harms an individual. Not all privacy breaches are interferences with privacy. A breach without harm is not an interference with privacy.

If the DHB breaches an individual's right to access their information this is also considered an interference with privacy - without the individual needing to show that they've been harmed as a result of the breach.

5.3 Lodging a complaint

DHBs should seek to address privacy complaints directly with the individual as much as possible, and while the Office of the Privacy Commissioner is always available to the individual, this should not be their first port of call to deal with their complaint.

However, any individual who thinks they have suffered a breach of the Privacy Principles or some other interference with their privacy can:

1. Lodge a complaint through ADHB's [Consumer Liaison Department](#).
2. Contact our Privacy Officer, [Sue Waters](#).
3. Complain to the Office of the Privacy Commissioner, (see <https://www.privacy.org.nz/your-rights/making-a-complaint/>).

6. Compliance, offences and fines

In some circumstances, failing to comply with this policy might be considered a breach of employment obligations and might be escalated to the Auckland DHB Human Resources Department for investigation and possible disciplinary procedures.

Refer to the Discipline and Dismissal policy (see [Associated documents](#)).

The Privacy Act 2020 gives the Privacy Commissioner greater powers to ensure businesses and organisations comply with their obligations. The following table provides the potential fines and actions that can be taken by the Privacy Commissioner for non-compliance:

Compliance and enforcement	Potential fines and actions
Access direction	<p>Principle 6 gives people the right to access their personal information. If a business or organisation refuses or fails to provide access to personal information in response to a principle 6 request without a proper basis, the Commissioner may now compel the agency to give this information to the individual concerned.</p> <p>Access directions may be appealed to the Human Rights Review Tribunal.</p> <p>The DHB can be fined up to \$10,000 for failing to comply with the access order.</p>
Compliance notices	<p>The Privacy Act 2020 allows the Commissioner to issue compliance notices to agencies that are not meeting their obligations under the Act. A compliance notice will require an agency to do something, or stop doing something, in order to comply with the Privacy Act. Compliance notices may be appealed to the Human Rights Review Tribunal.</p>
Refusing to comply with a compliance notice	<p>Refusing to comply with a compliance notice is an offence under the Privacy Act. A business or organisation that has been issued a compliance notice and fails to change its behaviour accordingly can be fined up to \$10,000.</p>
Misleading an agency to get personal information	<p>There is a new fine of up to \$10,000 for misleading a business or organisation to access someone else’s personal information. For example, it will be an offence to impersonate someone else in order to access their personal information.</p>
Destroying requested information	<p>If someone requests their personal information and a business or organisation destroys it in order to avoid handing it over, the business or organisation can be fined up to \$10,000.</p> <p>This includes inadvertent destruction of information; no matter to whom an individual may make a request for their information within the DHB, the DHB is responsible for processing that request and not destroying the information requested, even if it is two separate parts of the DHB responsible for each.</p>
Failing to notify a privacy breach	<p>If a business or organisation commits a privacy breach that has caused or is likely to cause serious harm, it must notify the Privacy Commissioner. Failing to inform the Commissioner of a notifiable privacy breach can result in a fine of up to \$10,000.</p>

7. Privacy impact assessments/ Privacy by design

7.1 Completing a Privacy Impact Assessment (PIA)

Where a proposed project, policy, service change or facility design or build may affect the collection, storage, security, access, retention, use and disclosure of personal or health information, the service must assess the privacy risks at the earliest opportunity.

A Privacy Risk Assessment flowchart and Privacy Impact Assessments (PIA) are tools to help identify and mitigate privacy risks being introduced to the DHB due to the change in the process/ system/ facility or service.

The service undertaking or proposing the change must complete the Privacy Risk Assessment flowchart to determine whether a full Privacy Impact Assessment is required. Based on the flowchart, a recommendation is provided as to whether a full Privacy Impact Assessment is required and why.

All Privacy Risk Assessment flowcharts and Privacy Impact Assessments must be reviewed for privacy and security considerations and endorsed by the Auckland DHB Privacy Officer and the Information Governance and Privacy Group.

To understand what is required or what needs to be considered when reviewing a PIA see Government Chief Privacy Officer (GCPO) website (see <https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/assess-privacy-risk/assess-project-privacy-risk/>) and review the 'Reviewing a Privacy Impact Assessment' section.

7.2 Privacy by design

The seven principles for Privacy by Design - and the philosophy and methodology they express — can be applied to specific technologies, business operations, physical architectures, networked infrastructure, and entire information ecosystems. The foundation is that privacy is built-in as the 'default setting'. Privacy is embedded throughout the product or service lifecycle from design to disposal. Further information can be found at the Government Chief Privacy Officer (GCPO) (see <https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/manage-a-privacy-programme/privacy-by-design-pbd/>).

8. Research, audit, quality assurance and quality improvement

All research projects should be registered with the Auckland DHB's Research Office. The Auckland DHB Research Office will review the proposal and provide the necessary approvals. Should the project require the use of identifiable personal information, Health and Disability Ethics Committees (HDECs) approval may be required. Please contact the Auckland DHB Research Office (see <https://www.adhb.health.nz/health-professionals/research/>).

Quality Assurance, Quality Improvement and Audit projects should be registered with the Clinical Records Department (see http://adhbintranet/HIMS/Clinical_Records/requesting_clinical_records.htm#VRAM_requests).

9. Support and administration

9.1 Roles and responsibilities

Protecting personal and health information requires support and vigilance from all DHB personnel. Some roles and responsibilities are defined, refer to [Appendix 1](#): Detailed Roles and Responsibilities for detailed information.

9.2 Training

DHB personnel must have an appropriate level of understanding of the legal and professional requirements governing the use of personal and health information. DHB personnel must complete the privacy training/ learning on Ko Awatea. Further e-learning modules are offered by the Office of the Privacy Commissioner (see <https://privacy.org.nz/tools/online-privacy-training-free/>).

9.3 Queries and complaints

If you have queries about the handling of personal or health information or this policy, please contact the Auckland DHB Privacy Officer, [Sue Waters](#).

All serious concerns and complaints about privacy and complaints alleging a breach of the Privacy Act 2020 or Health Information Privacy Code 2020 must be directed to the [Auckland DHB Consumer Liaison Team](#).

10. Supporting evidence

New Zealand Government. Social Investment Agency. 2019. Data Protection and Use Policy. Supporting the respectful, trusted and transparent use of people's data and information. December 2019 | Version 1.0.

11. Legislation

- Crimes Act 1961
- Evidence Act 2006
- Family Violence Act 2018
- Health (Retention of Health Information) Regulations 1996.
- Health Act 1956
- Medicines Act 1981
- Mental Health (Compulsory Assessment and Treatment) Act 1992
- Misuse of Drugs Act 1975
- Official Information Act 1982

- Oranga Tamariki Act 1989
- Privacy Act 2020
- Public Records Act 2005

All legislation available via legislation.govt.nz.

Other

- Code of Health & Disability Services Consumers' Rights
(see <https://www.hdc.org.nz/your-rights/about-the-code/code-of-health-and-disability-services-consumers-rights/>)
- Health Information Privacy Code 2020
(see <https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/hipc2020/>)

12. Associated documents

- Privacy Breach Guideline
- Clinical Record Management
- Information Privacy and Security Policy
- Discipline and dismissal

13. Disclaimer

No guideline can cover all variations required for specific circumstances. It is the responsibility of the health care practitioners using this Auckland DHB guideline to adapt it for safe use within their own institution, recognise the need for specialist help, and call for it without delay, when an individual patient falls outside of the boundaries of this guideline.

14. Corrections and amendments

The next scheduled review of this document is as per the document classification table (page 1). However, if the reader notices any errors or believes that the document should be reviewed **before** the scheduled date, they should contact the owner or [Document Control](#) without delay.

Appendix 1: Detailed roles and responsibilities

Role	Responsibilities
<p>Privacy Officer</p>	<ul style="list-style-type: none"> • Chair of the Information Governance and Privacy Group • Responsible for the privacy policy, strategy and programme of work. • Protects and promotes privacy by encouraging compliance with the Privacy Act 2020 and related Health Information Privacy Code 2020. • Conduct privacy incident investigations as necessary and prepare investigation summary reports. • Analyse breach information to assess organisational impact, if applicable. Responsible to communicate and consult on significant breaches with the Chief Medical Officer and Legal Team, as appropriate. • Responsible for reporting privacy concerns and updates to Senior Leadership Team. • Oversee external and internal communication and information sharing in the event of a privacy breach or incident. • Provide advice on privacy related matters, including requests for access, release and correction of personal information, privacy impact assessments and where potential privacy breaches have been identified. • Manage external relationships with the DHB Privacy Officer Group, Government Chief Privacy Officer and the Office of the Privacy Commissioner.
<p>DHB Employees</p>	<p>Understand and ensure compliance with the privacy principle requirements, managing personal information safely and with integrity – including:</p> <ul style="list-style-type: none"> • Restrict access by unauthorised personnel to areas where personal information is being stored. • Securely store files in unattended offices by either locking files in a cabinet or locking the office itself and do not leave any files unattended in public spaces. • Lock screens whenever any device is left unattended. • Ensure that all documentation in transit is placed in a sealed pouch or envelope. • Keep personal and health information away from public counters. • Encrypt or password protect any device that accesses any Auckland DHB network or holds any health or DHB related personal information. • Ensure that any DHB personal or health information that is taken off the premises is transported in a locked file or case or by encrypting information carried on a portable storage device.

Role	Responsibilities
	<ul style="list-style-type: none"> • Not disclose any DHB personal or health information on any message left on voicemail. • Never share personal login details with anyone. • Report any near miss or actual breach of privacy through Datix and notify senior manager and Privacy Officer immediately.
Chief Digital Officer	Responsible for implementing security functions to ensure electronic health information is adequately secured against loss and protected against unlawful access, misuse and disclosure
Corporate Records	<ul style="list-style-type: none"> • Responsible for the management of corporate records, with consideration for privacy and security. • Responsible for ensuring information is stored securely and appropriately with access restricted to an as-needs basis.
Executive Leadership Team	<ul style="list-style-type: none"> • Managing privacy awareness within their respective directorates. • Responsible for the governance and accountability of the District Health Board in relation to privacy and the Government’s Chief Privacy Officer’s expectations.
DHB Team Leaders/Managers	<ul style="list-style-type: none"> • Are responsible for the identification and initial response to privacy breaches. • Ensure team members complete the required privacy training in Ko Awatea. • Support and promote adherence to DHB privacy policies and procedures • Report all breaches or near misses through the formal incident reporting process. Where allocated, investigate the cause of the breach and provide recommendations for remediation. • Notification of the privacy breach or near miss to the Privacy Officer.
Human Resources	<ul style="list-style-type: none"> • Manage and safeguard staff records, include appropriate storage; user access and use. • Responsible to manage the disciplinary process, where required as defined by Auckland DHB’s internal policies.
Legal Team	<ul style="list-style-type: none"> • Providing legal advice on the interpretation and application of the Privacy Act and Health Information Privacy Code. • Providing legal representation on the Information Governance and Privacy Group (IGPG).
Information Governance and Privacy Group (IGPG)	<ul style="list-style-type: none"> • Support the DHB to meet its legal obligations under the Privacy Act 2020 and Health Information Privacy Code 2020. • Direct and oversee the implementation of the DHB’s Privacy Strategy. • Lead the development and implementation of policies, procedures, guidelines and security measures that aim to protect personal information, including health information.

Role	Responsibilities
	<ul style="list-style-type: none"> • Review and provide advice in relation to privacy related reports including summary or trend reports relating to privacy KPIs or privacy breach management. • Lead the development and implementation of privacy related training and education across the DHB. • Oversight of privacy risks, controls and assurance and related trends. • Identify and manage privacy maturity improvement opportunities and monitor the implementation thereof.
Clinical Records Department	<ul style="list-style-type: none"> • Perform user access reviews to ascertain appropriateness of access. • Manage the release of patient information as per the DHB procedure/ guideline. • Escalate any technical patient information release issues or enquiries to the Privacy Officer or Legal Team for further consultation, as required.
Research Committee/ Office	Responsible for the consideration of privacy and ethical aspects of research conducted at the DHB.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982