Title: 3DHB Privacy	
Type: Policy	**HDSS Certification Standard** (Optional)
Issued by: IPSC and DDIGG Committees	**Version:** 1
Applicable to: All DHB personnel HVDHB, WrDHB, CCDHB	**Contact person:** Privacy Officer CCDHB Chief Legal Officer CCDHB
Lead DHB: CCDHB	**Level:** 3DHB

Purpose:

This policy:

- Provides guidance to staff and confirms the DHB's expectations regarding the management of health and all other personal information, including the collection, storage use and disclosure of the information.
- Outlines our compliance requirements with the 13 Privacy Principles as defined in the Privacy Act 2020 and the Rules of the Health Information Privacy Code 2020.

Scope:

This policy applies to all DHB personnel who handle or manage personal information.

> While this policy refers to "health information" and "patients", the rules and requirements contained within it are equally applicable to other types of personal information such as personal information relating to employees and contractors of the DHB.

Guiding Values:

The following guiding values support this policy:

- Ready access to and sharing of accurate health information is essential for the provision of appropriate clinical care and treatment.
- 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 kaitiaki[1] 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.

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

- 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.
- This policy includes considerations from the Data Protection and Use Policy (DPUP). We acknowledge and incorporate the Data Protection and Use Policy values of *He tāngata; Manaakitanga; Mana whakahaere; Kaitiakitanga;* and *Mahitahitanga* into all privacy practices.

Definitions:

Term	Definition
DHB personnel	Is 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.
Health information	Means personal information about medical history, disability or health services provided to an individual. This includes information about both a living individual and a deceased individual.
Information	Includes: • written material (including medical records, test results, correspondence, emails, meeting minutes and notes of verbal discussions) • data recorded or stored on any tape-recorder, computer, device, or portable storage device • graphs or drawings • photographs, films, negatives, tapes or other devices in which visual images or audio recordings are capable of being reproduced (including diagnostic images)
Individual	Is a natural person, such as DHB personnel, a patient or a visitor.
Personal information	Information about a living identifiable individual.[2] Examples of personal information include an individual's name, telephone number, address (email and postal), date of birth, ethnic origin, 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 Principles	There are 13 privacy principles contained in the Privacy Act 2020. Where this

[2] A National Health Index (NHI) on its own does not constitute personal information.

Term	Definition
	policy refers to a principle, it will be written as **PPn** (n=number)
Third Party (includes other agencies)	Is 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 or Oranga Tamariki), or other individuals (such as whanau or family of a patient).

Policy content

Why do we need a Privacy Policy?

- The DHB plays a privileged and trusted role as kaitiaki and guardians of individuals' health information. Because of this role, THE DHB places privacy at the core of how we work with the public.
- The DHB also has a large number of employees and our staff expect us to safeguard their employee information.

The aim of this policy is to ensure that our systems, processes and practices provide a comprehensive and sound platform to safeguard personal information so that all staff manage the personal information we hold in a knowledgeable and respectful manner.

What do we need to do?

Collect only the information necessary to carry out our functions and responsibilities. [PP1] We collect patient health information for the predominantly for the purpose of providing care and treatment, but also for administrative, training and education and monitoring quality of care. Personal information relating to DHB personnel is collected for determining job suitability, work performance, workplace health and safety, workforce planning and administration. Further guidance can be found in the Collection Personal Information Guideline.

Collect information, where possible, directly from the individual [PP2] We will collect information straight from the individual and will also, in some situations, collect information from other people such as next of kin or who have the individual's consent or authority to act on their behalf. Further guidance can be found in the Collection Personal Information Guideline.

Make people aware of the collection of their information [PP3]. We will inform individuals of why their information is being collected, who will see it, whether collecting is voluntary and what will happen if it is not collected. Further guidance can be found in the Collection Personal Information Guideline.

Collect information in a way that is lawful, fair, open and transparent. [PP4] We will take extra care to ensure that children and young people are showed additional respect and care

when we collect information from them. Further guidance can be found in the Collection Personal Information Guideline.

Store information with reasonable safeguards against loss or misuse [PP5] See Appendix 1 of this policy for a list of the physical, operational and technical measures we are all expected to take to protect personal and health information while in use, storage and transit.

Ensure all individuals have the right to access their personal and health information and to seek to correct it if it's wrong [PP6 and PP7]. We acknowledge that everyone has a legal right to make a request to the DHB for access to their information and to seek to correct it if it is wrong. The rights to access and correct are not, however, automatic. Further guidance on when access or correction may or may not be allowed can be found in the procedures on An Individual's right to access their own personal information and the Request for the Correction of Personal Information.

Take steps to ensure personal and health information is complete, relevant, and up to date.[PP8] We will take reasonable steps to check that information is accurate before it is used. For further guidance refer to the Information and Records Management Policy.

Destroy the information once it has served the purpose for which it was collected. [PP9] Personal and Health information should be stored for only as long as it is necessary for the purpose it was collected. Health information must be retained under certain legislation such as the Health (Retention of Health Information) Regulations 1996 and the Public Records Act 2005.

Establish a clear and lawful purpose for collecting personal information, and use and disclose it according to that purpose [PP10]. Personal and health information should generally be used for the same purposes it was collected. Further guidance can be found in the Collection Personal Information Guideline and the Use and Disclosure of Personal Information Guideline

Disclose personal or health information to other parties only where there is legal authority to do so [PP11]. THE DHB may disclose personal or health information to third parties to fulfil our legislative obligations and protect the health and safety of individuals. The DHB will take reasonable steps to ensure third parties protect the personal and health information the DHB shares with them in line with legislation and with the same care the DHB gives to it. Further guidance can be found in the Use and Disclosure of Personal Information Guideline and the Privacy Impact Assessment (PIA) Procedure

Disclose personal information to an overseas recipient only if it is safe to do so for the individual [PP12]. Disclosure to overseas recipients can occur if that entity meets one of the requirements as outlined in PP12. If they do not, then disclosure should not occur unless the individual authorises it. For further guidance please refer to Appendix 2 of this policy and the Privacy Impact Assessment (PIA) Procedure .

Use a unique identifier (such as an NHI) only for the purpose for which it was created and only where necessary [PP13]. Any unique identifier created for one purpose may not be used for another.

Ensure privacy is considered for all new or changed systems that involve personal information.

Complete privacy impact assessments (PIA) in all new business process developments where personal information is involved. Further guidance can be found in the Privacy Impact Assessment (PIA) Procedure

Respond quickly and appropriately to a privacy breach or incident. Further guidance can be found in the Dealing with a Privacy Breach procedure.

Provide training, resources and guidance material on privacy practices and health information management. New staff are trained to ensure the privacy principles are applied when fulfilling their role within THE DHB. Existing staff are regularly trained on privacy risk areas specific to their business area, as well as broader privacy principles. Further guidance can be found in the [Link to e-learning Privacy programme]

Protect the privacy of staff members. Staff personal and health information is treated with the utmost care and respect, and in accordance with the Privacy Act 2020. Further guidance can be found in the Employee Information Policy.

Who is responsible?

Protecting personal and health information across the DHB requires the support and vigilance from all staff. Defined roles and responsibilities of the DHB staff are listed in Appendix 4 of this policy.

What happens if I breach this Policy?

The DHB's Code of Conduct sets out the expectation that staff will comply with all policies and procedures. Actions found to be in breach of the Code of Conduct may result in disciplinary action. Any privacy breach which also amounts to an interference with a person's privacy may result in the DHB liable for compensation payments.

What happens if the DHB breaches the Privacy Act?

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 against an agency for non-compliance:

Compliance and enforcement	Potential fines and actions
Access direction	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 compel the agency to give this information to the individual concerned. The DHB can be fined up to $10,000 for failing to comply with the access direction.
Compliance notices	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.
Refusing to comply with a compliance notice	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.
Misleading an agency to get personal information	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.
Destroying requested information	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. 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.
Failing to notify a privacy breach	If a business or organisation has 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.

Where can I seek help?

The DHB's Privacy Officer can provide support or respond to any complaints about privacy related matters under the Privacy Act or Health Information Privacy Code.

References:

National Privacy Working Group	A National DHB Privacy working group was established to offer a nationally consistent approach by DHBs to the changes to the Privacy Act 2020. This policy has adopted and drawn from that National Policy. View the National DHB Privacy Policy 2020 here.
NZ Legislation	Privacy Act 2020 Health Information Privacy Code 2020 Official Information Act 1982 Health Act 1956 Public Records Act 2005 Vulnerable Children Act 2014
Data Protection & Use Policy	The Data Protection and Use Policy (DPUP) articulates what 'doing the right thing' looks like across the social sector in its collection and use of people's data and information. DHBs are not legally bound by the DPUP, but are encouraged to consider it when collecting, using and sharing information. The policy comprises five principles, *He tāngata* – focusing on improving people's lives; *Manaakitanga* – upholding the mana and dignity of the people; *Mana whakahaere* – empowering people by giving them choice; *Kaitiakitanga* – acting as a responsible steward; *Mahitahitanga* – working as equals to create and share knowledge. For further information see the Social Wellbeing Agency's website here.

Appendices:

Appendix 1 Storage and Security of Information

Appendix 2 Disclosing Information to overseas recipients Guide

Appendix 3 Summary of the Privacy Act principles

Appendix 4 List of Roles and Responsibilities

Appendix 1 – Storage & Security of Information

Safeguarding and securing information is the responsibility of all THE DHB staff who handle patient health and other personal information.

Physical security

Staff are expected to:

- 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;
- Lock computer screens whenever a device is left unattended;
- Cover names on files when they are in transit around the hospital;
- Not display health information on the outside of envelopes such as the name of the department from which the letter is sent;
- Keep personal and health information away from public counters;
- Be considerate when collecting or discussing sensitive health information in a setting which allows others to overhear the conversation;
- Ensure that personal and health information is held in a secured filing cabinet or office and not left in trolleys in corridors during clinics;
- Encrypt or password protect any THE DHB or personally owned or controlled portable storage device that accesses THE DHB network or holds THE DHB health information;
- Not download nor store THE DHB personal information on any personally owned or controlled portable storage device.

Operational Security

Staff are expected to:

- Avoid e-mailing personal information to external e-mail addresses. Where sensitive personal information must be e-mailed, the email can be encrypted, or the sensitive information can be sent by way of a password protected attachment. (Contact ICT Service desk if you need assistance);
- Ensure that any personal information taken off the premises is kept secure, such as in a locked file or case; or by encrypting information carried on a portable storage device;
- Not disclose health or personal information on phone answering machines;
- Avoid using faxes to transmit personal information.

Technical security

Staff are expected to:

- not share login details with anyone;
- not leave a computer terminal unattended without locking the screen

Appendix 2 – Disclosing Information to an Overseas Recipient

Only disclose information overseas if it is safe to do so for the individual – [Principle 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).

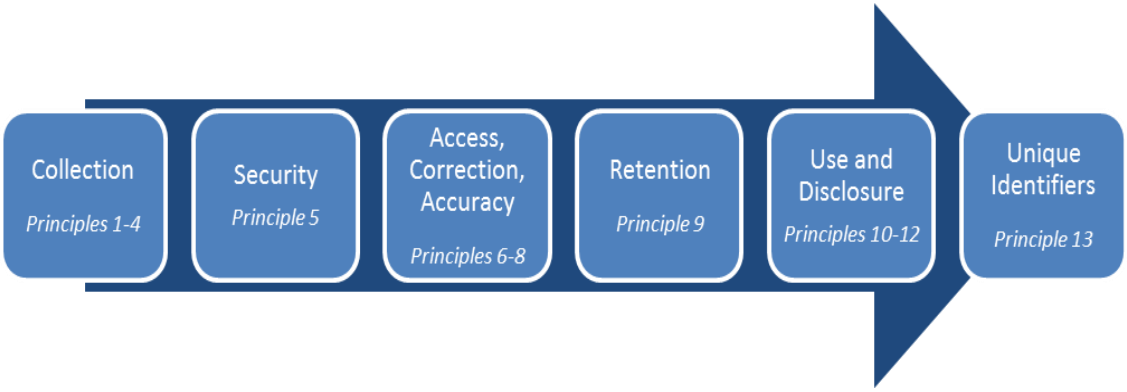
Sending information to an overseas cloud storage service to hold information on the DHB's behalf is not considered to be an overseas disclosure of information, as the storage service is holding the information on behalf of the DHB for safe custody under section 11 of the Privacy Act 2020.

The Privacy Act 2020 has extraterritoriality 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.

Appendix 3 – Privacy Act Principles

To protect and respect personal information, the following principles apply:



Principle 1 – Only collect personal information if you really need it

The DHB must collect information that is necessary for the present or anticipated purposes of the agency.

Principle 2 – Get it straight from the people concerned where possible

We should aim to get personal information directly from the person to whom it relates. Sometimes that isn't practical, such as where the person is unconscious or getting it from them would undermine the reason you're collecting it. Those examples are covered in the Privacy Act as appropriate exceptions.

Principle 3 – Tell them what you're going to do with it

We should aim to tell the person, as soon as we have collected information from him/her why it is being collected; who will see the information; if they have to give the information or whether this is voluntary; and what will happen if they don't provide the information. Sometimes we can't tell a person these things, for example, if the person is unconscious at the time of collection, but that is an accepted exception under the Privacy Act.

Principle 4 – Collect it legally and fairly

Personal information must not be collected by unlawful means or by means that are unfair or unreasonably intrusive in the circumstances such as by hidden cameras.

Principle 5 – Take care of it once you have got it

It's impossible to stop all mistakes, but agencies must ensure that there are reasonable safeguards in place to prevent loss, misuse or disclosure of information without authority.

Principle 6 –People can see their personal information if they want to

People have a right to ask for access to that personal information. However, sometimes agencies can refuse to give access to information, for instance where giving the information

would endanger a person's safety or involve an unwarranted breach of someone else's privacy.

Principle 7 – They can correct it if it is wrong

People have a right to ask the agency to correct information about them if they think it is wrong. If the agency doesn't think correction is warranted, they can offer to have the person add *their* views to the record.

Principle 8 - Make sure personal information is correct before you use it

An agency must take reasonable steps to check that information is accurate before it is used.

Principle 9 – Get rid of it when you are done with it

An agency must not keep information for longer than is necessary for the purpose(s) for which they collected it.

Principle 10 - Use it for the purpose you got it

Agencies must use personal information for the same purpose for which they collected it. Other uses are sometimes permitted, such as where it's necessary to enforce the law, or the use is directly related to the purpose for which the agency got the information.

Principle 11 - Only disclose it if you have a good reason

Agencies can only disclose personal information in limited circumstances. An agency can disclose information if it reasonably believes, for example that: the person concerned authorises it; the information is going to be used in a form that does not identify the person; disclosure is one of the purposes for which the agency got the information in the first place; disclosure is necessary to prevent or lessen a serious threat to the life or health of an individual.

Principle 12 - Only disclose information overseas if it is safe to do so for the individual

Principle 13 - Only assign unique identifiers where permitted

A patient's NHI is an example of a unique identifier as it is a means of identifying someone without use of their name. An agency cannot use a unique identifier given to a person by another agency.

Appendix 4 – Roles and Responsibilities

[To be adapted by each DHB]

Individual	Accountability
All Staff (includes volunteers and contractors)	Understanding and ensuring compliance with the privacy principle requirements; Managing personal information safely and with integrity. Respecting others' information and being mindful when discussing personal information that it is appropriate and in the correct forum. Being familiar with THE DHB's privacy policies and procedures.
Chief Digital Information Officer	Responsible for: Implementing security functions to ensure electronic health information is adequately secured against loss and protected against unlawful access, misuse and disclosure.
Information Management Adviser	Responsible for: Leadership for effective management and use of information across THE DHB; Provision of advisory services supporting staff; Contributing IM expertise at a corporate level, through the Information Governance Group, and the Information Privacy and Security Group; Developing a sustainable IM Programme across THE DHB..
Executive Leadership Team	Responsible for: 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.
Human Resources	Managing and safeguarding staff records, including appropriate storage; user access and use. Managing the disciplinary process, where required as defined by THE DHB's internal policies.
Legal Team	Responsible for: Providing legal advice on the interpretation and application of the Privacy Act and Health Information Privacy Code. Providing legal representation on the Information Privacy and Security Governance Group. Supporting the Privacy Officer. Ensuring the DHB's policies and procedures comply with the Act and Code and other relevant legislation, including any

Individual	Accountability
	amendments, legal developments and case law.
Information Privacy Security Working Group	The role of the Group is to: 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. Direct and oversee the implementation of measures to ensure that personal information is managed in accordance with all relevant legislation as well as the DHB's policies and procedures. Lead the development and implementation of privacy related training and education across the DHB The Committee is responsible for: Supporting the DHB to meet its legal obligations under the Privacy Act 2020 and Health Information Privacy Code 2020; Approving Privacy Impact Assessments; Promoting good privacy management practices across THE DHB; Providing oversight of THE DHB's privacy practices; Actively informing improvements on privacy management across THE DHB; and Ensuring a consistent approach is taken to privacy related matters across THE DHB.
Patient Information Service	Responsible for: Releasing patient information as per THE DHB's procedures; and Escalating any technical patient information release issues or enquiries to the Privacy Officer or Legal Team for further consultation, as required.
ICT Service	Performing user access reviews to ascertain appropriateness of access.
Privacy Officer	Member of the Information Privacy Security Governance Committee. Responsible for: The privacy policy, strategy and programme of work; Protecting and promoting privacy by encouraging compliance with the Privacy Act and related Health Information Privacy Code; Conducting privacy incident investigations as necessary, and preparing investigation summary reports for IPSG;

Individual	Accountability
	Analysing breach information to assess organisational impact, if applicable. Communicating and consulting on significant breaches with the IPSG, Communications team, CEO, Chief Medical Officer and Legal Team, as appropriate; Regular monthly reporting to IPSG; Reporting to Executive Leadership Team, as appropriate. Overseeing external and internal communication and information sharing in the event of a privacy breach or incident; Managing external relationships with Government Chief Privacy Officer and the Office of the Privacy Commissioner.
Quality Managers	Supporting adherence to policy and procedure; Providing reports on breaches and near misses to Privacy Officer, as appropriate.
Research Committee/ Office	Membership at the IPSG; Responsible for considering privacy and ethical aspects of research and audit conducted at THE DHB.
All Staff in Management roles including Operations Managers; Clinical Leaders; Service Managers; Team Leaders and Line Managers	Responsible for: Identifying and providing initial response to privacy breaches; Reporting all breaches or near misses through the formal incident reporting process. Where allocated, investigating the cause of the breach and providing recommendations for remediation. Notifying the Privacy Officer of the privacy breach or near miss.