The Heart Group

PATIENT PRIVACY POLICY

At The Heart Group we are committed to protecting individual privacy and meeting our obligations under the Privacy Act 2020 ("**Act**") and the Health Information Privacy Code 2020 ("**Code**").

Who we are

For the purposes of this policy, "The Heart Group" ("we", "us", "our") includes:

- Individual cardiologists practising at The Heart Group;
- The company Intra Limited; and
- All employees, and contractors (including clinical, technical, nursing, and administrative staff.)

Scope of this Policy

This policy explains how we collect, use, store, disclose, and protect personal and health information (together referred to as "**Information**") in providing healthcare services.

Collection of Information

We collect your information only where it is necessary to provide healthcare services to you, including to support your diagnosis, treatment, and ongoing care, and to manage and support the safe and effective delivery of those services. We collect information lawfully, which includes in a manner that is fair, and doesn't unreasonably intrude on your privacy.

We may collect Information:

- directly from you;
- indirectly from, for example:
  - other healthcare providers and organisations involved in your care, such as your GP, other specialists, hospitals, and diagnostic providers (including laboratories and radiology services). This may include Information shared through referral letters, clinical reports, test results, or shared electronic health record systems (such as TestSafe, a secure Health New Zealand system used to share test results);
  - funders of your care such as ACC, insurers and government agencies; and
- your family or whānau with your consent.

What we tell you

Direct collection (IPP 3 / Rule 3)

When we collect Information directly from you, we take reasonable steps to ensure you are aware of:

1. the purpose of collection;
2. the intended recipients;
3. the name and address of The Heart Group;
4. whether the supply of Information is voluntary and the consequences of not providing it;
5. your rights to access and request correction; and
6. any legal authority for the collection (where applicable).

This information is generally provided through our **Privacy Consent Form**.

Indirect collection (IPP 3A / Rule 3A)

Where we collect Information from another source, we take reasonable steps to ensure you are aware that your Information has been collected and who it has been collected from, and of the matters listed

at (1) – (6) above. This notification is provided within a reasonable timeframe after collection, unless an exception applies.

For routine and expected indirect collections, this notification is generally achieved through our **Privacy Consent Form** and admission processes, which explain that we may collect Information from other providers and external agencies involved in your care. By signing the Privacy Consent Form, you confirm that you have read and understood this, and agree to the collection, use, and disclosure of your Information as described.

In some cases, Information may be collected indirectly outside the usual channels described in the Privacy Consent Form and this Policy (for example, from family members, employers, or other third parties not involved in routine care pathways). Where The Heart Group retains or uses this Information, we will notify you of that collection. Because this type of indirect collection is not covered by our standard notification framework, notification will generally be provided on a case-by-case basis, in accordance with Rule 3A.

In some situations, we may not need to provide notice, including where:

1. you are already aware of how your Information will be collected and used (for example, through your referring doctor or our Privacy Consent Form);
2. it would be unreasonable or impracticable to notify you of the collection of the Information;
3. informing you of the collection of the Information could prejudice yours, or another persons, health or safety; or
4. we are otherwise permitted not to do so under the Privacy Act or the Code.

Purpose of collection and use

We collect and use your Information to:

- Provide diagnosis, treatment, and ongoing care;
- Coordinate referrals and services;
- Communicate with you and other providers involved in your care;
- Manage administration, billing, and insurance claims;
- Support quality assurance and service improvement;
- Respond to feedback, concerns and complaints;
- Comply with our legal, regulatory, and contractual obligations.

We only use your Information for: these purposes, a directly related purpose, another purpose with your consent, or as otherwise permitted or required by law.

Use of electronic systems

We use secure electronic systems to manage Information and support aspects of your care (e.g. clinical record systems, scheduling, and administration). These include shared electronic health record systems, which can be accessed by us and other external healthcare providers.

These systems assist staff, however all clinical decisions are made by qualified health professionals.

Disclosure and intended recipients

We may disclose Information where permitted by the Act or Code, including:

- For the purposes for which it was collected or a directly related purpose (refer above);
- To healthcare providers involved in your care, including Health New Zealand;
- To diagnostic and treatment providers;
- On electronic health records systems shared with other healthcare providers, including TestSafe;

- To relevant funders (e.g. ACC, insurers, government agencies);
- For administrative, billing, claims and debt recovery purposes;
- Where necessary to prevent or lessen a serious threat to health or safety;
- Where the information is in a form that does not identify you;
- Where otherwise required or authorised by law.

Storage, security and retention

We take reasonable steps to protect your Information from loss, unauthorised access, use, or disclosure, including through:

- Secure systems and access controls;
- Confidentiality obligations for staff and contractors;
- Monitoring and audit processes.

We retain Information only as long as necessary for its lawful purpose and in accordance with legal retention requirements, after which it is securely disposed of.

Access, accuracy, and correction

You have the right to request access to, and correction of, your Information.

We take reasonable steps to ensure Information we hold is accurate, up to date, complete, and not misleading.

Requests should be made to our Privacy Officer. We will respond in accordance with the Act and provide reasons if a request is refused.

Overseas disclosures

We disclose Information overseas only where permitted by the Act, including where comparable privacy safeguards are in place, or you have authorised the disclosure.

Third parties

Access to Information by third-party service providers is limited to what is necessary for them to perform services for us. All third-party service providers are required to maintain appropriate privacy, confidentiality, and security safeguards, and are contractually bound to protect Information in accordance with applicable privacy laws.

Unique identifiers

We use National Health Index (**NHI**) numbers to support accurate identification and continuity of care.

Privacy breaches

We maintain processes to identify, manage, and respond to privacy breaches.

Where we become aware of a privacy breach, we will assess whether the breach is likely to cause serious harm to any affected individual.

If the breach is assessed as likely to cause serious harm (a notifiable privacy breach), we will comply with our obligations under the Privacy Act 2020, including:

- Notify the Privacy Commissioner; and
- Notify affected individuals as soon as practicable (unless an exception applies).

In assessing whether a breach is likely to cause serious harm, we take into account relevant factors, including the nature of the information, the likelihood of misuse, and the steps taken to mitigate any risk.

We will take all reasonable steps to contain the breach and reduce the risk of harm.

Any suspected privacy breach should be reported to our Privacy Officer as soon as possible.

Privacy Officer and contact details

Privacy Officer: Suzanne Endicott-Davies.
Email: suzannee@heartgroup.co.nz
Phone: 09 623 6373
Address: 1 Gilgit Road, Epsom, Auckland

Concerns or complaints

If you have a privacy concern or complaint, please contact our Privacy Officer.

We investigate and respond as soon as practicable. You may also contact the Office of the Privacy Commissioner.

Policy Updates

We update this policy from time to time. The latest version will be available on our website.