**HealthLink Privacy Notice for New Zealand**

Healthlink is committed to delivering high privacy standards that protect, support and empower the privacy rights of health service consumers and comply with Privacy Laws. Below we have provided a description of how we integrate this philosophy into our service design and delivery.

**Our privacy protocols**

Our suite of services is built on a desire to ensure that health information / service requests are conducted in a manner that protects the privacy of the individuals involved and complies with the privacy laws. We're consumers of health services too, and we would want our information to be treated respectfully – therefore, we apply that same standard to our processes.

Here we have provided you with detailed explanations regarding how we ensure your personal information is treated in accordance with privacy legislation.

| Privacy principle | Our approach |
|---|---|
| Principle 1 – Purpose for collection | We ensure that personal information collected is necessary and for a lawful purpose related to the provision of services we deliver.<br>Our business purpose is to enable the secure exchange of health information to enable providers to deliver better care to their patients. These exchanges occur between authorised health service providers and other organisations such as government agencies and insurance organisations. Examples of these exchanges include completing claim forms for ACC, or sending referrals to specialists; and therefore, personal information included can include relevant medical information such as diagnoses, consultation notes, specialist reports.<br><br>We also capture product improvement data when authorised organisations and health providers use our solution. This data does not contain personal information and is used for purposes of issue resolution, service delivery, and product improvement. For example, it may include analyses of transaction volumes and delivery timeframes.<br><br>Finally, we also capture personal information such as names and phone numbers of health providers that use our services. This information is collected and used to enable core business functions of service delivery, helpdesk support, billing and service reporting. |
| Principle 2 – Source of information | The specialist nature of our data exchange service does not require us to collect personal information direct from individuals. Our service exists for situations where the personal information required for the authorised organisation's business purpose cannot be collected directly from the individual (e.g. obtaining detailed medical history or performing a medical exam). |
| Principle 3 – what to tell an individual | Through this Privacy Statement, our contracts and business processes we ensure that when organisations and providers use our service, they have obtained sufficient informed consent from their clients. This includes being clear about what information will be collected, who will access it, who it will be shared with, whether it is |

| | |
|---|---|
| | voluntary, what will happen if the info isn't collected, and what purpose this collection is enabling. |
| Principle 4 – Manner of collection | We ensure that information exchanges through our solution are done so in a way that is fair, reasonable and respectful towards clients and all individuals concerned. |
| Principle 5 – Storage and security | We have strong technology and processes in place that ensure only authorised individuals necessary to perform our legitimate business purpose can access personal information.<br>All health information stored in our system is encrypted. |
| Principle 6 – Access;<br>Principle 7 – Correction; and<br>Principle 8 - Accuracy | We fully support an individual's right to request a copy of their personal information that we hold, and we will do what we can under the Privacy Act to enable this in a respectful and speedy way.<br><br>We will first do a system check to identify what personal information we have on file.<br><br>Following that, the Privacy Act requires us to take reasonable efforts to ensure that releasing this information will not cause harm to anyone at all. For this part of this process, we might do a quick check with the doctor who provided the information, and we will also potentially speak with the agency that has requested the copy of the information in the first place.<br><br>Please note that in line with our data retention policy we may have already deleted your personal information collected by us; and in cases where we haven't deleted the information, any medical information will be encrypted and thus inaccessible by us. That said, any information securely delivered through our platform should be available from the organization that shared it via our solution.<br><br>Where possible we are happy to correct any information that is inaccurate. We also take reasonable steps to ensure that the info we receive is accurate. This relates only to personal details (e.g. surname, or date of birth) that are used by the health providers to identify you. If we see a potential error in these (e.g. we might identify a possible typing error in a common surname) we will confirm first with the requesting organisation. |
| Principle 9 – Retention | We delete personal and health information from our system in adherence to our Data Retention Schedule or under the instruction of our customers. For example, we have invested in our technology to apply rules that automatically delete messages and forms sent through our HMS solution within 30 days of them being delivered to the recipient.<br><br>Note that after deletion the information exchanged through our system is potentially still available to the person that sent it, through their own system (e.g. your GP will have a copy of referrals in their practice mgmt. system). |

| | |
|---|---|
| Principle 10 – Use | Our purpose is to allow health information to be exchanged securely and quickly. Our job is to enable the smooth and secure transfer to the authorised organisation. |
| Principle 11 – Disclosure | Information we gather through our service delivery is only accessible directly from our service by those authorised to access it. In most cases secure exchanges are delivered into the recipients' systems, at which point their own internal processes take over. We also have a secure online portal via which some providers access exchanges sent to them. Access to this portal is protected by strong security standards. |
| Principle 12 – Disclosure of personal information outside of NZ | We do not make any disclosures of personal information to offshore entities |
| Principle 13 – Unique identifiers | We do not assign a unique identifier to individuals. |

**Management of cookies in our website**

Please refer to our overarching Clanwilliam Health policy here.

**If you have a privacy complaint about Healthlink**

If you have any concerns about how we manage your personal information, you may contact the Healthlink Privacy Officer at privacy@healthlink.net