Laura Fergusson
Brain Injury Trust

Policy – Privacy

Laura Fergusson Brain Injury Trust

Policy – Privacy

Contents

1. Statement

The Laura Fergusson Brain Injury Trust (LFBIT) provides high-quality clinical care and community rehabilitation that help support clients who are affected by stroke, traumatic and acquired brain injury, spinal injury, post-surgical recovery, and neurological conditions such as Multiple Sclerosis.

This Policy sets out how LFBIT will ensure all Client and Employee Information is managed in accordance with LFBIT and Employees' legal, ethical, and professional obligations. This Policy:

a) Establishes the framework by which LFBIT and Employees will manage Information and protect Individual's privacy.

b) Sets out obligations and responsibilities that LFBIT and Employees must meet to comply with their legal obligations in the Privacy Act (PA), Health Information Privacy Code (HIPC), and other relevant legislation in relation to Personal and Health Information collected and held by LFBIT.

c) Sets out how LFBIT will manage an actual or potential privacy breach.

This Policy should be read in conjunction with the Security of Information Framework for more information about operational and technical aspects of how LFBIT ensures Personal, and Health Information is stored securely and for governance relating to Information security.

2. Scope

This Policy applies to all Information held by LFBIT, including Personal Information about Employees and Health Information about Clients. It applies to all Employees and Board members, and any other person or organisation dealing with Personal or Health Information, in any format, including electronic information, on behalf of LFBIT. This includes volunteers, students, and contractors (refer to definition of Employee in this Policy). This policy also covers all databases and personal information held by Laura Fergusson Foundation.

3. Responsibility

All LFBIT Staff, Board members, and any other person to whom this Policy applies are responsible for ensuring they understand and meet their obligations and responsibilities under the PA, HIPC, other relevant legislation, and this Policy.

Information security governance arrangements are established and endorsed by the LFBIT Board and assisted by other quality committees. More information on these responsibilities is found in the Security of Information Framework.

4. Definitions

Client	Any person receiving services or care from any LFBIT service.
Employee	Means all LFBIT current and former employees, Board members, persons providing services under contract to LFBIT, volunteers, students and any other person involved in LFBIT operations.
Information	Includes Personal Information and Health Information. Information is not limited to written information but includes any knowledge gained or held, including for example in written notes, emails, audio or CCTV recordings, and photos.
Health Information	Has the same definition as in the HIPC. It includes all information about an identifiable individual obtained while providing health and disability services, including: • information about the health of that individual, including his or her medical history • information about any disabilities that an individual has, or has had • information about any health services or disability services that are being provided, or have been provided, to that individual • information provided by that individual in connection with the donation, by that individual, of any body part or any bodily substance of that individual or derived from the testing or examination of any body part, or any bodily substance of that individual; or • information about that individual, which is collected before or during, and incidental to, the provision of any health service or disability service to that individual addresses, billing information and information related to funding.
Personal Information	Has the same definition as in the PA and means information about an identifiable individual.
Representative	Representative is defined in the HIPC to mean: d) The executor or administrator of a deceased person's estate; the parent or guardian of a person under 16 (whether the person is alive or dead); e) Where a person is alive and over 16 but is unable to give consent or exercise his or her rights, someone who seems to be lawfully acting on the person's behalf (such as someone with an enduring power of attorney for personal care and welfare, or welfare guardian) or in his or her interests (such as a friend or relative).
Staff	Relates to LFBIT staff members only and does not include volunteers, students, or contractors.
Artificial Intelligence apps (e.g. ChatGPT, Bing)	AI encompasses a wide range of techniques and approaches aimed at developing intelligent systems. These techniques have developed over time and together, these contribute to the advancement of artificial intelligence language model's (AILM's) such as ChatGPT.

5. Confidentiality obligations

The LFBIT will ensure all Personal and Health Information is managed in a confidential manner. Confidentiality is the explicit undertaking by Employees and Board members to keep information that they have access to as part of their role or involvement with LFBIT confidential and to only collect, use, or share the Information appropriately and in a manner that meets their legal obligations under the PA and HIPC and as set out in this Privacy Policy.

Health professionals must also meet their ethical and professional obligations of confidentiality. All Employees and Board members must sign a confidentiality agreement and must abide by the requirements set out in this agreement.

Employees and Board members confidentiality obligations continue after they leave the role or employment or stop providing services to LFBIT.

Maintaining appropriate confidentiality of Personal and Health Information is important and includes in the working environment, where services are being provided, in personal conversations, and at social functions. All Employees and Board members must be aware of, and abide by, their obligation of confidentiality. This includes:

a) Only authorised Employees are entitled to access Personal and Health Information during their roles and duties with LFBIT

b) Clients' Health Information must only be accessed, used, or shared to provide the Client with health and disability services, and as otherwise set out in this Policy

c) All Health or Personal Information must only be accessed and used by an Employee to perform their duties as an Employee, and must only be shared with persons entitled to know the Information;

d) Employees must take appropriate care to ensure that Personal and Health Information is not accessible to unauthorised persons.

Any breach of this Policy and an Employee's obligations under this Policy, including their confidentiality obligations is serious. In relation to Staff, a breach may amount to serious misconduct under the Code of Conduct and may result in immediate dismissal. In relation to other Employees a breach may result in discontinuance of the Employee's services or relationship with LFBIT.

6. Purposes for which LFBIT collects Information

LFBIT collects Health Information to enable us to provide our clients with safe and effective health and disability services. This includes:

a) To ensure we identify Clients properly so that all Information is uniquely identifiable to the intended Client

b) To assess Clients needs effectively so we can work with our clients to provide clinically and culturally safe and effective health and disability services, care and treatment;

c) To provide required treatment, care, advice and other health and disability services

d) To ensure appropriate and timely coordination across service providers so our clients receive safe and effective ongoing care

e) To meet all legislative and contractual requirements

f) To administer and manage the services we provide, including charging, billing and debt collection for business and operational purposes

g) To maintain and improve the quality of our services through quality improvement activities, audit and monitoring, and training

h) To enable us to respond and manage complaints and concerns.

i) Clinical data be used for large-scale 'audit' group research; no personal information (e.g., name, date of birth, photo, NHI number) will be reported.

We also collect Personal Information about Employees to meet our legislative and contractual requirements, and for other lawful purposes including:

a) For Employee selection and vetting

b) For monitoring work performance and conduct at work and to ensure Employees' work performance, and activity is not impaired by any work or non-work-related activities

c) To ensure LFBIT meets its legal obligations relating to health and safety in the workplace including ensuring that an Employee does not pose a hazard to him or herself or to others

d) To ensure LFBIT meets all legislative and other legal obligations in relation to Employee information (for example under the Holidays Act, providing relevant information to Inland Revenue and so on)

e) For contractual management and review

f) For quality assurance, audit, and training purposes to support LFBIT operations and the safe and effective provision of care, advice, treatment and rehabilitation to our Clients

g) For security purposes.

7. Rules in the Health Information Privacy Code and Information Privacy Principles in the Privacy Act

7.1 Collection of Information (Rules 1-4, IPPs 1- 4)

Strict rules apply to the Information LFBIT may collect about Clients and Employees. In particular:

a) LFBIT will only collect Information where it is necessary for a lawful purpose connected with LFBIT functions and activities

b) LFBIT will collect Information directly from the Client or Employee unless one of the exceptions in rule 2 of the HIPC or IPP 2 of the PA allows LFBIT to collect the Information from another source.

In most cases the Client or Employee should know when LFBIT is collecting Information about them. They should also be informed about the purposes for which their Information may be used, when the Information may be shared, and who has access to their Information. The person can then make a choice whether to provide the Information or not and will not be surprised later with how their Personal or Health Information is used or disclosed.

If a client or Employee declines to provide Information the person concerned should explain to the Client or Employee, the reasons why the Information is being sought and the possible consequences of not providing the Information. For example, this might include that a particular service or treatment may not be able to be provided or to continue effectively without complete and accurate Information. If the Client or Employee has applied for a benefit or subsidy it may not be possible to take action to process the claim without the requested Information. However, once this explanation has been provided the Employee or Client's right to refuse to provide the Information should be respected.

In appropriate circumstances LFBIT may obtain Client Health Information from a shared care database.

LFBIT informs Clients of when and how their information is collected and may be used or disclosed by way of its Privacy Statement. This is provided to all Clients on admission to the service as part of our Informed Consent process. Employees are informed of this Policy during their induction to employment with us and via the bi-annual mandatory training.

The HIPC and PA allow for non-compliance with the collection rules in the HIPC and PA in some circumstances. Some of the exceptions that might apply to LFBIT include:

a) The Client or Employee authorises the collection from someone else

b) Collecting the Information from the Client or Employee is not reasonably practicable in the circumstances. For instance, the Client may not know the Information, or may not be able to understand an explanation because of their mental or physical health, or you may need a family member's perspective on the effect of a particular medication etc.

c) Obtaining the information from the Client or Employee would undermine the purpose of collecting the Information

d) Noncompliance is necessary for the maintenance of the law or the conduct of proceedings before a court or tribunal

e) Compliance would prejudice the interests of the Client, the purpose of collection or prejudice any person's safety

f) Noncompliance would not prejudice the Employee's interest.

The exceptions are similar but different when it comes to an Employee's Personal Information (IPPs 2 and 3) and a Client's Health Information (rules 2 and 3 of the HIPC).

The Privacy Officer should be consulted where there are any concerns about whether or how Information should be collected.

Information must not be collected in a manner that is unfair or unreasonably intrusive. LFBIT will take care to ensure appropriate physical privacy when sensitive Information is being collected.

7.2 Unsolicited Information

The collection rules in the HIPC and PA do not apply to unsolicited Information. For example, where a family member rings LFBIT and provides information about a client without being asked by LFBIT or someone provides Information to LFBIT seen on a Facebook page about an Employee.

However, if LFBIT holds onto or uses or discloses the Information all the other rules in the HIPC and information privacy principles in the PA will apply (e.g., rules/IPPs 5 – 12).

7.3 Storage and security of information (Rule 5, IPP 5)

Maintaining appropriate security and confidentiality of Personal and Health Information is important to maintaining trust in LFBIT. Security of Information is based on the following five elements:

a) Confidentiality - ensuring that Information is only accessible to those with authorised access
b) Integrity - safeguarding the accuracy and completeness of Information and processing methods
c) Availability - ensuring that authorised users have access to Information when required
d) Compliant Use - ensuring that the processes meet all legal and contractual obligations
e) Responsible Use - ensuring that appropriate controls are in place so that users have access to accurate, relevant, and timely Information.

LFBIT takes reasonable steps to ensure the security and safe storage of Personal and Health Information it holds against loss, unauthorised access, modification, use or disclosure or any other misuse. LFBIT complies with NZS 8153:2002 (Health Records) and ensures appropriate security and protection of Personal and Health Information by the following methods. All Employees and Board members with access to Client or Employee Information are expected to be familiar with and comply with these controls.

a) **Physical and Environmental Management:** LFBIT applies measures to ensure that the level of physical controls implemented minimises or removes the risk of equipment or information being rendered inoperable or inaccessible, or being accessed, used, or removed without appropriate authorisation. The controls are set out in more detail in the Information Security Framework.
b) **Communications and operations management:** LFBIT will ensure that operational procedures and controls are documented and implemented to ensure that all Information assets and ICT assets are managed securely and consistently, in accordance with the level of required security. Each Staff member and where relevant, Employee, must use the LFBIT authorised and supplied communications methods, including electronic mail, when transacting official LFBIT business.
c) **Access management:** LFBIT has in place control mechanisms based on business requirements, assessed/accepted risks, Information classification and legislative obligations for controlling access to Personal and Health Information. Employees with access to the LFBIT cloud-based server must always log off each individual session on the server and never leave open their desktop email or other documents they are working on if they are not present at their desk.

Refer to the Security of Information Framework and the Finance and Administration Policy for more detailed information relating to how LFBIT ensures the security of Information and Employees obligations relating to storage and safeguarding Information against misuse, loss, and inappropriate access, use or disclosure of Personal and Health Information.

7.3.1 Client notes should not be removed from LFBIT premises

Client notes should not be removed from LFBIT premises except in exceptional circumstances. Where it is necessary to take Client records off site:

a) No more than the bare minimum of notes are to be taken away from the LFBIT facility (i.e., A Client's entire file should not be taken if you only need recent progress notes from the last session)
b) Client notes should be stored electronically where practicable
c) If taken off site a client notes should be kept in a locked compartment, regardless of whether the Employee shares a house with anyone (including their children).
d) If a client's notes must be left in a locked car, they must not be visible and must be in a locked boot.

7.3.2 Use of cellphones for Client Information

Employees should not use LFBIT cell phones for photographing Clients. An exception to this is where a photograph of a client undertaking some activity is necessary for treatment and assessment purposes. An example of this is where it is necessary to take a photograph of a client in a vehicle for a driving modification assessment. Employees are not permitted to use personal cell phones for this purpose.

Any images are to be saved within the LFBIT work environment (One Drive or Teams) on the employees LFBIT cell phone.

7.4 Access to, or correction of, Information (Rules 6 and 7, IPPs 6 and 7)

Individual Employees and Clients have a right to:

a) Know if LFBIT holds Information about them; and

b) Access that Information if it is readily retrievable; and

c) Ask for the Information to be corrected if they think it is wrong.

7.4.1 Access request

A request by a person for access to their own Information can be made orally or in writing and there is no requirement for the person to explain why they want their Information, or to say that they are making the request under the HIPC or PA.

In some situations, it may not be appropriate to provide all the Information requested. The only grounds for refusing to give a person access to their own Personal or Health Information are set out in IPP 6 of the PA and rule 6 of the HIPC. A request for access by a person for their own Personal or Health Information cannot be refused on the grounds that the person does not own the Information or has an outstanding debt to LFBIT.

If LFBIT receives a request for Personal or Health Information the Privacy Officer must be informed and will manage the request in accordance with the requirements in the PA. This includes, logging the request, determining with the senior health professional involved whether the requested Information is to be provided or whether any Information should be withheld, and ensuring the decision on the request is made as soon as reasonably practicable and within 20 working days as required under the PA.

This timeframe can only be extended, and some or all the requested Information can only be withheld if one of the limited reasons for an extension or withholding the Information set out in the PA applies.

In relation to a request from a client (or where relevant the Client's Representative) for a copy of all or some of their Health Information the Information should be reviewed by the senior health professional responsible for the Client's care before the Information is released. The request, and the actual Information released should be recorded in the Client's file.

7.4.2 Request for correction of Information

A person can also ask for their Personal or Health Information held by LFBIT to be corrected if they think the Information, or part of the Information is wrong.

LFBIT is under an obligation to ensure the Information it holds is correct. However, if LFBIT does not believe the Information is incorrect it does not have to correct the Information as requested. Information that was the honestly held opinion at the time should not be changed as removing or changing the Information may make the notes incomplete. However, LFBIT must give the person concerned an opportunity to add their views about what the correct information is to their Personal or Health Information record. LFBIT must then attach this 'statement of correction' to the Personal or Health Information in a way that it will be read with the disputed Information.

An access or correction request should be forwarded to the Privacy Officer in the first instance. The Privacy Officer will be responsible for logging the request and ensuring the actions LFBIT must take when it receives an access or correction request, set out in rules 6 and 7 of the HIPC and information privacy principles 6 and 7 of the PA, and the timeframe and obligations set out in the PA are met.

7.5 Ensuring information is accurate and up to date (Rule 8, IPP 8)

Before LFBIT uses information, it must take reasonable steps to ensure the Information is accurate, up-to-date, complete, relevant, and not misleading. What is reasonable will depend on who the Information was collected from, when the Information was obtained, and the proposed use or disclosure.

Care should be taken when the Information has been obtained from someone other than the person concerned. Consideration should be given as to whether it is appropriate to verify that Information with the individual concerned before the information is relied on.

7.6 Retention of information (Rule 9, IPP 9)

The Health (Retention of Health Information) Regulations requires LFBIT to retain Health Information for 10 years from the last date of treatment or care unless LFBIT transfers the Information to another provider or gives the Information to the person concerned.

Other laws may require Personal or Health Information to be retained for specific purposes. LFBIT must not keep Personal or Health Information for longer than is necessary for any lawful purposes it uses the Information for. LFBIT has processes in place to ensure it does not retain Personal or Health Information for longer than is necessary.

7.7 Use of information (Rule 10, IPP 10)

LFBIT will only use Personal or Health Information for the purposes for which it was collected. The exception to this is if one of the exceptions in information privacy principle 10 of the PA (for

Personal Information) or rule 10 of the HIPC (for Health Information) applies. The most common exceptions that may apply to LFBIT include:

a) Where the Client (or where relevant their Representative) or the Employee concerned has authorised the use (rule 10(a), IPP 10(b))

b) Where the other use is directly related to the purpose for which the Information was collected (rule 10(b), IPP 10(e))

c) Where that use of the Information is necessary to prevent or lessen a serious threat to the life or health of the person concerned or any other person or to public health or safety (rule 10(c), IPP 10(d)),

d) Where necessary to avoid prejudice to the maintenance of the law or the conduct of proceedings before a court or tribunal (rule 10(f), IPP 10(c))

e) The information is de-identified or will be used in a form which the Client or Employee concerned is not identified (rule 10(e) or IPP 10(f).

In the event that a client does not have capacity to consent to treatment or services, LFBIT will need to provide relevant Information about the Client to the individual legally entitled to consent on the Client's behalf. This is necessary to obtain informed consent from the person legally entitled to consent for the Client. LFBIT will take reasonable steps to ensure it correctly understands who has legal authority to consent on behalf of a client who lacks the capacity to consent for themselves and will retain this legal authority in the Client's clinical file.

The Privacy Officer should be consulted before information is used for a purpose other than for which it was obtained and where the individual concerned has not authorised the new use.

7.8 Disclosing Client or Employee Information (Rule 11/IPP 11)

LFBIT will only disclose a Client's Health Information or an Employee's Personal Information if:

I. The Client or Employee authorises the disclosure

II. The disclosure is a purpose for which the Information was collected

III. Any other exception in rule 11 of the HIPC or IPP 11 of the PA applies

IV. Any other law requires or authorises the disclosure.

The requirements for disclosure of Health Information under the HIPC are more stringent than for Personal Information under the PA. Before a disclosure of a Client's Health Information is made in reliance on any of

the exceptions in rule 11(2) of the HIPC the Client's authorisation should be obtained for the disclosure unless it is not practicable or desirable to obtain the authorisation.

Disclosure under one of the exceptions in rule 11 or IPP 11 is discretionary, and LFBIT has a choice whether to disclose the Information or not. If LFBIT does decide to disclose Information only necessary Information should be disclosed, and the Information must be disclosed securely to the correct person or agency. LFBIT will take reasonable steps to ensure any Information disclosed is correct and up-to-date and that any such disclosure follows the requirements in the HIPC, PA, or the law requiring or permitting the disclosure and this Policy.

The process LFBIT follows when responding to a request for a client or Employee's Information from another agency or organisation is set out in the **flow diagram in appendix 1**. All requests for a Client's Health Information should be in writing (email is fine) and state the reason for the request, the actual Information requested, why it is necessary for the organisation to obtain the Information, and if the organisation does not want the request disclosed to the client the reason for this.

The Privacy Officer should be consulted before Information is disclosed unless the disclosure is authorised by the Client, or it is a purpose for which the Information was collected

7.9 Situations where LFBIT may want to disclose, or may be requested to disclose Information

7.9.1 Client or Employee authorises disclosure or disclosure is a purpose of collection

Health Information can be disclosed under rule 11 if the Client (or where relevant their Representative) authorises the disclosure, or the disclosure is for one of the purposes for which LFBIT collected the information and the Client was aware of that purpose. These disclosures are part of the normal procedures and include such things as:

a) Disclosing information to other members of the care or treatment team such as occupational therapists, the GP, pathology, or radiology where tests have been ordered, the Client's hospital specialist

b) Disclosing information to a contact person to assist with care for the Client (who the Client has authorised to receive the information);

c) Referring the Client, with their agreement to another provider or service.

In the same manner, Personal Information about an Employee may be disclosed with the Employee's authorisation or where the disclosure was a purpose of collecting the information and the Employee was aware of this. An example would be providing relevant information to the Employee's chosen kiwisaver provider or Information related to making their salary payment into their nominated bank.

Information may also be disclosed for a purpose directly related to a purpose for which the Information was collected, for example for services being provided or treatment of a client, or for a purpose directly related to the purpose an Employee's Information was collected. This should be a purpose that the Client or Employee would reasonably expect as part of their ongoing care or working relationship with LFBIT (rule 11(2) (a) or IPP 11(a)).

7.9.2 Disclosure to family, caregivers, and friends

If the Client (or where relevant their Representative) authorises the Information to be shared with family members, caregivers, or any other person the Information may be shared. If the Client (or where relevant their Representative) has not authorised the sharing of the Information with a family member or support person/friend their authorisation should be sought before the Information is shared.

The HIPC also allows disclosure of a Client's Health Information to the Client's principal caregiver, near relative or nominated contact person without the Client's consent where it isn't desirable or practicable to seek consent under (rule 11(2)(b)). Disclosure under this exception can only be made by a Health Practitioner registered under the Health Practitioners Competence Assurance Act; must be in line with recognised professional practice; and must not be disclosed if the Client vetoes the disclosure.

7.9.3 Request for Information from a caregiver providing services to the Client

If a Client's caregiver requests Health Information about the Client, the request must be dealt with under section 22F of the Health Act. See further information about requests under s22F of the Health Act below.

7.9.4 Disclosure to a Client's Representative (section 22F of the Health Act and rule 11 HIPC)

If a client is unable to exercise his or her rights under the HIPC, or is deceased, LFBIT may disclose Information to the Client's 'Representative' (as defined in the HIPC and see below) (rule 11(1)(a)(ii)).

The Client's Representative can also request the Client's Health Information under s22F of the Health Act in which case there are limited grounds for refusing the request.

The following persons may be a Client's Representative:

I. If the Client is deceased, the administrator or executor of the estate

II. If the Client is under 16 years of age, his or her parents or guardians

III. If the Client is alive and 16 years or older and is unable to give consent or exercise their rights under the HIPC, a person appearing to be lawfully acting on his or her behalf or in his or her interests. This will include a person who holds an enduring power of attorney for personal care and welfare (EPOA for personal care and welfare), a welfare guardian or a Court appointed guardian.

If a Client's Representative requests Information, the Information must be disclosed unless LFBIT has reasonable grounds for believing that:

I. The disclosure would be contrary to the Client's interests; or

II. The Client does not, or would not, want the Information disclosed; or

III. One or more of the reasons for refusing to disclose the Information set out in section 27-29 of the Privacy Act apply.

If none of these exceptions apply, the Information must be disclosed in accordance with the request.

If any of the above do apply, then the request may (but does not have to) be refused. However, if the request is refused, the Representative may complain to the Privacy Commissioner, and he/she must be told of this right.

7.9.5 Disclosing Health Information to other health and disability providers

It is important that there is appropriate co-operation among organisations and health professionals providing health and disability services to Clients to ensure quality and continuity of services (Right 4(5) of the Code of Rights). This may require the sharing of relevant Information with other providers when necessary for the Client's care or treatment. In this case the disclosure would be for one of the purposes for which the Information was collected, and the Client should have been made aware of this.

Providers who are, or who are about to provide health or disability services to the Client may also request relevant information from LFBIT. This is a request under section 22F of the Health Act. Relevant Information must be provided following such a request unless one of the reasons for refusing the request set out in the PA and rule 11(4) of the HIPC applies (see further information above). Where it is practicable and desirable the Client's consent should be sought before the Information is provided following a request. Refer to the flow diagram for requests for a Client's Information in Appendix A.

7.9.6 Requests from other organisations (Te Whatu Ora, PHOs, Police, Oranga Tamariki, Medical Officer of Health, Health and Disability Commissioner and so on)

Where another agency or organisation requests Information about a Client or Employee LFBIT should only disclose the Information if:

I. The Client or Employee authorises the disclosure

II. One of the exceptions in rule 11 or IPP 11 applies; or

III. There is another law that **allows** or **requires** the Information to be disclosed. In this case disclosure of **relevant Information** covered by the other law will not breach the HIPC.

Examples where LFBIT may be permitted or required to disclose a client or Employee's Information **following a request** include:

I. To another health or disability service provider, or person providing health or disability services to the Client (section 22F of the Health Act).

II. To the police. Disclosure following a request from the police is only mandatory if the police have a search warrant or production order. Police may also request Health Information relating to a Client under section 22C of the Health Act. If LFBIT has any concerns about the scope of a search warrant or production order it should seek immediate legal advice before any Information is provided.

III. To Te Whatu Ora. A Te Whatu Ora employee may request Health Information for the purposes of undertaking their powers and functions under the New Zealand Public Health and Disability Act under s22C of the Health Act.

IV. To the Ministry of Social Development (including WINZ). The Ministry of Social Development has powers to require Information under s 11 of the Social Security Act. However, these powers must be exercised proportionately and in accordance with the MSD Code of Conduct and do not give the Ministry the right to collect all Information about an Employee or Client.

V. To Oranga Tamariki. An Oranga Tamariki social worker or Care and Protection Coordinator can request relevant Health Information under s22C of the Health Act and under the information sharing provisions in the Oranga Tamariki Act (discussed further below).

VI. Anyone has a discretion to make a report of concern to Oranga Tamariki or the police under s 15 of the Oranga Tamarki Act if they are worried that a child or young person could be, or is being, harmed, ill-treated, abused, neglected, or deprived in any way or otherwise have concerns about their wellbeing. For further information on sharing information regarding preventing a risk of harm to, or the wellbeing of, a child or young person with appropriate agencies see the section below on information sharing under the Oranga Tamariki and Family Violence Acts.

7.9.7 Disclosure of a serious risk of harm or to prevent prejudice to the maintenance of the law

Information may be disclosed where the disclosure is necessary to prevent a risk of **serious threat to the life or health** of the person concerned or any other person or to **public health or safety.**

Any disclosure must be to a person who is able to do something real about the risk (rule 11(2)(d) and rule 11(3) or IPP 11(f)), and only relevant Information should be disclosed.

Information may also be disclosed voluntarily or following a request where the disclosure is necessary for court or tribunal proceedings (rule 11(2)(i), or IPP 11(e)). The disclosure must be made to the relevant agency, court or tribunal and only relevant Information should be disclosed.

Where LFBIT wants to, or has been requested to, disclose Health Information under these exceptions it must first consider whether it is desirable or practicable to seek the Client's consent to the disclosure.

7.9.8 Children under 16 years of age

Parents or guardians of children under 16 years of age are their Representative under the HIPC. This means they are entitled to request information about their child (until the child's 16th birthday) under section 22F of the Health Act. However, this right is not absolute as there will be circumstances where it is not appropriate or safe to disclose a child's Health Information to a parent or guardian. The Information must be provided unless:

I. The child does not or would not want the Information disclosed

II. It would not be in the child's interests to disclose the Information

III. One of the other grounds for refusing to disclose the Information in sections 27 – 29 of the PA applies.

If there is any doubt that it is in the child's interest to release the Information, either voluntarily or following a request from a parent or guardian, the information should not be released without further advice from the Privacy Officer.

A parent or guardian may continue to be a Representative of their living child when the child is over 16 years of age if, the child is unable to give consent or exercise their rights under the HIPC, and the parent or guardian is acting on the child or young person's behalf or in his or her interests (refer to the definition of Representative in the HIPC). This would include where the child does not have the capacity to consent to health or disability services or treatment and the parent or guardian retains their guardianship right to consent on their behalf (up to the child's 18th birthday).

7.9.9 Requests for disclosure of a deceased Client's Information

Under the HIPC and Health Act the only persons entitled to request a copy of a deceased Client's Health Information is the 'personal representative' of a deceased person (refer to definition of Representative in the HIPC). A 'personal representative' means either an executor of the will or, if there is no will, an administrator of the person's estate. If the requestor is not either the executor of the Client's will or, if there is no will, an administrator of the Client's estate they will not be entitled to access the Client's Health Information.

If the requestor is the executor of the Client's will or administrator of their estate LFBIT can only refuse the request if it has reasonable grounds for believing the Client did not or would not wish their Health Information to be disclosed (22F(2)(c) of the Health Act and rule 11(4)(b)(ii) of the HIPC).

A Client's enduring power of attorney for personal care and welfare (EPOA for personal care and welfare) ceases to have effect on the death of the Client. Therefore, unless the person holding the EPOA for personal care and welfare is also the executor of the Client's will or administrator of their estate they will not be entitled to request a copy of the deceased Client's Health Information. A Client's next of kin or close family members also do not have any right to access the deceased Client's Health Information.

7.9.10 Disclosure where the Client or Employee is not identifiable

Information may be disclosed if it is to be used in a form that does not identify the Client or Employee concerned (rule 11(2)(c) or IPP 11(h)). This exception can only be relied on if it is not practicable or desirable to obtain the client's authorisation. Section 22H of the Health Act also permits the disclosure of "anonymised" Health Information that does not permit the identification of the Client to whom it relates. If any of these exceptions are relied on care must be taken that the Information is truly non-identifiable.

7.9.11 Disclosure Overseas (IPP 12)

IPP12 – Disclosures outside NZ only permitted if:

Individual authorises the disclosure

Recipient subject to Privacy Act 2020 or privacy laws that provide comparable safeguards

Recipient part of a prescribed binding scheme

Recipient subject to privacy laws of a prescribed country

Recipient otherwise subject to arrangements that ensure the information is subject to comparable safeguards

8. Artificial Intelligence (AI) use

AI apps such as ChatGPT are being used in the workplace for several reasons such as

- Text generation: used as a starting point for tasks such as drafting reports, presentations, proposals, and developing business strategies by using its natural language generation capabilities to provide data driven insights and recommendations.
- Automating desktop research; by generating summaries, providing relevant insights, and identifying key findings from large volumes of text-based data such as reports, articles, and academic papers

LFBIT employees must be aware that the same rules apply (under the Privacy Act 2020) when utilizing AI applications and staff members must not upload any client data into ChatGPT or similar app as this would be unauthorized disclosure of client related information and in breach of the Privacy Act.

AI must not be used for storing or sharing confidential client / health information, storing public records or client records.

Staff using AI must also be aware of breaching copyright or intellectual property rights.

9. Information sharing under the Oranga Tamariki and Family Violence Acts

New and amended information sharing provisions came into force in July 2019 to enable appropriate sharing of Information in circumstances where a child or young person may be at risk of harm, ill-

treatment, abuse, or neglect or in family violence situations. These provisions are found in the Oranga Tamariki and Family Violence Acts.

9.1 Information sharing to a Child Welfare and Protection Agency (CWP Agency) or 'Independent Person'.

The information sharing provisions in the Oranga Tamariki Act allow CWP Agencies and some Independent Persons (as defined in the Act) to request, use, and share relevant Information for specific purposes related to the well-being and safety of a child or young person (up to their 18th birthday). Information may be shared with appropriate CWP Agency and an Independent Person if it is to:

I. Prevent or reduce the risk of harm, ill-treatment, abuse, or neglect of a child or young person

II. Make or contribute to an assessment of the risks or needs of a child or young person

III. Make, contribute to, or monitor any support plan for a child or young person that is managed by Oranga Tamariki.

CWP Agencies are defined in s2 of the Oranga Tamariki Act and include many welfare, support, justice, health, education, transport, policing, and local authority services.

'Independent Persons' is defined in s2 of the Oranga Tamariki Act to mean:

I. Health Practitioners registered under the Health Practitioners Competence Assurance Act who provides health and disability services

II. A Childrens worker (as defined in s23(1) of the Children's Act);

III. And a person or class of persons designated as an independent person by regulations under s 447(1) (ga)(ii) of the Oranga Tamariki Act.

Any proposed sharing of Information under these provisions must be for one of the purposes set out in the Act and must come within the provisions of the Act. Helpful guidance on sharing information under these provisions is available at:

https://www.orangatamariki.govt.nz/working-with-children/information-sharing/.

9.2 To a Family Violence Agency (FV Agencies) or a Social Services Practitioner.

The information sharing provisions in the Family Violence Act allows sharing of Information to:

I. Help protect the victim from family violence

II. Make or contribute to family violence risk or need assessment

III. Make decisions or carry out plans related to responding to family violence.

FV Agencies and Social Services Practitioners are defined in the Family Violence Act to mean:

I. **FV Agencies:** Includes specified government agencies, Te Whatu Ora, School Boards and licensed early childhood services, and NGOs that are partially or wholly funded by the government to provide family violence services.

II. **Social Services Practitioners:** Means health practitioners registered under the Health Practitioners Competence Assurance Act, Social Workers Registration Act, and teachers who hold a current practising certificate who are providing health, disability, or education services.

Under the Family Violence Act there is also a new **duty** on FV Agencies and Social Services Practitioners to **consider** sharing relevant Information with an appropriate FV Agency or Social Services Practitioner if it may help protect a victim of family violence, or if the FV Agency or a Social Services Practitioner receives a request for information for a permitted purpose under the FV Act. This is **not** a mandatory reporting requirement but does require FV Agencies and Social Services Practitioners to consider sharing relevant Information relating to family violence.

10. Managing a privacy breach

If a breach of privacy occurs, LFBIT will follow the steps set out for responding to a breach in the Privacy Commissioner's Guidelines and guidance on responding to a privacy breach. These steps include:

Step 1: Containing the breach and making an initial assessment

Step 2: Evaluating the risks associated with the breach

Step 3: Notification. Once the risk associated with the breach have been identified consider who should be notified, including:

a) Persons' who's Personal or Health Information has been lost, stolen or misused.

b) The Privacy Commissioner

Changes to the Privacy Act expected to come into force late 2019 or 2020 are likely to require mandatory reporting of privacy breaches where there is a risk of serious harm. If this change to the legislation comes into force LFBIT will comply with the mandatory reporting requirement and will follow any guidance published by the Privacy Commissioner.

Step 4: Prevention – Consider what lessons can be learned to prevent future breaches.

These steps will be taken as soon as reasonably practicable. The Privacy Officer must be notified as soon as practicable and will lead the response to the breach.

The Privacy Officer is also responsible for:

a) Establishing and maintaining a privacy breach/information security incident and response register and a Privacy Breach Plan. All privacy breach incidents will be recorded on the register and will be managed in accordance with this plan and the current Guidance from the Office of the Privacy Commissioner.

b) Ensure LFBIT meets all requirements under the PA and HIPC when responding to and managing a privacy breach.

c) Ensure all privacy breach or information security incidents are reported and escalated (where applicable) in a timely manner, through appropriate management channels and/or authorities. Ensure that these incidents are investigated and if it is found that a deliberate security violation or breach has occurred, apply formal disciplinary processes.

11. The role of the Privacy Officer

The Privacy Officer is responsible for:

a) Ensuring that LFBIT, Employees comply with their obligations under the PA in relation to Employees, and the HIPC in relation to Clients; and

b) Dealing with requests made to LFBIT about Personal or Health Information in compliance with the procedural provisions and timeframes in the PA and other relevant legislation; and

c) Facilitating on-going training for all Staff on their obligations under the PA and HIPC and this Policy; and

d) Managing any privacy breach or complaint that may occur, including working with the Privacy Commissioner or investigating officer should the need arise and undertaking the actions set out under Managing a Privacy Breach in section 14 of this Policy.

Associated Documents

Consumer Rights Policies

HR Policies and Procedures

Finance and Administration Policy

Security of Information Framework Policy

LFBIT Disaster Recovery Plan.

Privacy Act 1993 (Amended 2020)

Health Information Privacy Code 1994

On the Record, a Practical Guide to Health Information Privacy 2nd edition.

Health Act 1956

Health (Retention of Health Information) Regulations 1996

Oranga Tamariki Act 1989

Family Violence Act 2018

NZS 8153:2002 (Health Records)

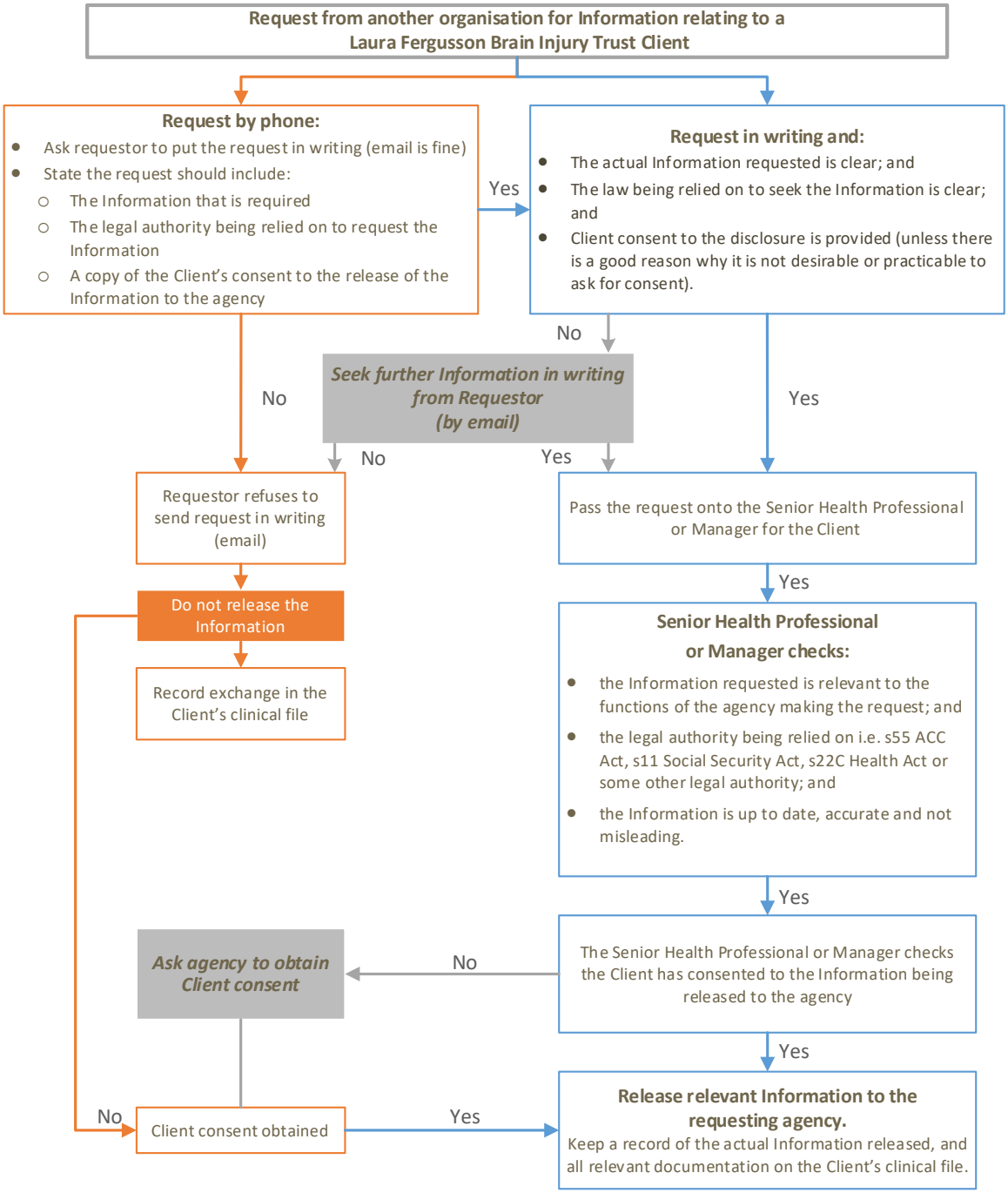
Distribution List

Https://LFTcant.sharepoint.com/

LFBIT Website www.lfbit.co.nz

Appendix 1

Requests for Client Information from another organisation



NOTES

The Privacy Act enables agencies to collect, use, and disclose information that is necessary and proportionate to their lawful requirements. An agency's authorising legislation may provide a mechanism by which the agency can require Information to be provided from persons other than the individual. However, usually Information should be sought directly from the individual concerned, unless there are reasonable grounds to believe that this would 'prejudice the maintenance of the law' or another exception in rule 11 of the HIPC applies.

LFBIT should not release information without the consent of the Client except in exceptional circumstances where it is not practicable or desirable to obtain the Client's consent. If the requesting agency considers the Client's consent should **not** be sought, for instance because it would jeopardise the purpose for collecting the information, it should provide LFBIT with a clear explanation.