PRIVACY POLICY

Statement

Everyone at Anxiety New Zealand Trust plays a part in helping develop and promote a culture in which personal information is protected and respected.

Links

The new Privacy Act 2020 came into force on 1 December 2020, with a revised Health Information Privacy Code (HIPC) 2020 alongside it. You can read more here:

- Independent explanation about the new Privacy Act 2020.

- The Privacy Act 2020

- Information on the Health Information Code 2020

Scope

The Privacy Policy covers all personal information that we collect, use, disclose or store. This includes belonging to or relating to:

- Anxiety NZ Employees and Volunteers

- People accessing clinical, peer, helpline and other Anxiety NZ Trust services.

- Complainants and other members of the public

Definitions

Personal Information contains values that identifies a specific individual.

Standards

Collection:

We collect personal information from you, including information about your:

- name
- contact information
- location
- interactions with us
- billing or purchase information
- health information
- NHI number for the purpose of reporting PRIMHD data to the MOH and medication prescriptions.

We collect personal information in order to:

- provide mental health services, support and education

Providing some information is optional. If you choose not to share relevant mental health information that impacts our ability to provide appropriate and quality care, we'll review whether we can safely

provide support or if we will to provide decline services in which case we may refer you to another service.

Storage and Security

We keep your information safe by storing it securely and only allowing certain staff to access it.

As required by Clause 5 of Health (Retention of Health Information) Regulations 1996 Anxiety NZ keeps clinical information from accessing health services for a minimum of 10 years. When information is destroyed this is done by confidential shredding of any hard copy materials, and or deletion of data from our servers. For further clarification visit: AskUs | Article | How long do medical records have to be kept for? | Office of the Privacy Commissioner

Access and Correction

You have the right to ask for a copy of any personal information we hold about you, and to ask for it to be corrected if you think it is wrong. If you'd like to ask for a copy of your information, or to have it corrected, please contact us at, or +649846 9776, or 77 Morningside Drive, St Lukes, Auckland, 1025.

Use and Disclosure

Personal information is only to be used for the purpose(s) for which it was collected, unless there is good reason to use it for other purposes and this is allowed by the Privacy Act 2020. If there is any doubt about the purpose for which personal information was collected or is being used, the Privacy Officer is to be consulted

Personal information about an individual is to be provided only to that individual or to other individuals or organisations they have authorised us to provide their information to, except where required or authorised by law. Where a request for an individual's information is received, Anxiety NZ's privacy officer can provide advice as to whether this information should be provided.

Before information is used or disclosed, it is to be checked to the extent possible to ensure that it is accurate, complete, up to date and relevant. Limits on disclosure of information apply to disclosure to other people and teams within Anxiety NZ as well as to external organisations. Relevant personal information may be disclosed by staff internally if it is consistent with the purposes for which it was collected. A process for monitoring access to personal information and identifying inappropriate access is being implemented.

Releasing personal information to a third party is permitted provided that the procedures relating to this are accurately followed. We will provide personal information to other people or organisations if we need to do so to deliver our functions, and with consent or where required or authorised by law.

We may disclose personal information, with appropriate safeguards in place, to:

- Approved employees or Volunteer Workers of Anxiety New Zealand Trust who have appropriate safeguards in place. These safeguards may include Confidentiality Agreement, Code of Ethics and Conduct Agreement, Vulnerable Persons Declaration and Annual Police Checks and may also include appropriate current registrations to bodies such as the Medical Council, Psychotherapists, Psychologist or Counselling Board.

- Health care professionals, Community Mental Health Services, vocation education & advisory bodies, or other agencies providing information for the purposes of consideration of conduct and competence

- Our business and service providers (such as IT providers)

- Our professional advisors (such as insurers and auditors)

- Government and regulatory authorities, where required or authorised by law (including the Health & Disability Commissioner, ACC, Police, overseas equivalents of the Medical Council) and with appropriate documented agreements in place.

Examples of safeguards for disclosure of information include memoranda of understanding with external organisations, confidentiality agreements, secure means of transfer, and/or assurance over the information handling practices of external organisations. The Privacy Officer should be consulted in all new situations of personal information disclosure.

We are required to take all reasonable steps to ensure third parties protect personal information with the same care and respect we do. The memoranda of understanding in place are part of this process and must be adhered to.

Privacy Breaches and Incidents

A privacy breach refers to unauthorised access to or collection, use or disclosure of personal information. It is 'unauthorised' if it is not in compliance with the Privacy Act 2020 and the Health Information Privacy Code (HIPC) 2020.

Under the Privacy Act 2020, there is a privacy breach that is likely to cause anyone serious harm, The Privacy Officer or other nominated person at Anxiety NZ must notify the Privacy Commissioner and any affected people as soon as practically able. The Notify tool may be used to work out of a privacy breach is notifiable or a Breach may be directly notified to the Privacy Commissioner by The Privacy Officer or other nominated person at Anxiety NZ using a Privacy Breach Notification Form.

All staff must notify their Manager immediately if a privacy incident is suspected or identified. The Privacy Officer must also be notified the same day of the privacy breach.

Anxiety NZ has a 'no blame' policy and there will not be any repercussions for a privacy breach as long as the incident was accidental, reasonable care was applied, and Anxiety NZ policies and procedures have been followed. However, disciplinary action may follow if:

- There is a deliberate breach of an individual's privacy.

- Any deliberate disclosure of personal information for purposes other than specified in this policy is considered serious misconduct.

- A privacy breach is covered up or attempted to be hidden.

Not immediately notifying their manager or Privacy Officer is considered serious misconduct.

- Avoiding or circumventing Council policies or systems which results in a privacy or security breach whether intentionally or unintentionally.

- Where a reasonable level of care is not applied when carrying out a function or your role or task assigned to you that involves personal information and a breach occurs.

- Repetitive privacy breaches.

Accountability and Responsibility

The CEO is responsible for developing and maintain a culture of privacy that reflects Anxiety New Zealand's values.

The Privacy Officer (CEO) duties are:

- be familiar with the privacy principles in the Privacy Act
- work to make sure the organisation complies with the Privacy Act
- deal with any complaints from the organisation's clients about possible privacy breaches
- deal with requests for access to personal information, or correction of personal information
- act as the organisation's liaison with the Office of the Privacy Commissioner.

They may also:

- train other staff at the organisation to deal with privacy matters
- advise their organisation on compliance with privacy requirements
- advise their organisation on the potential privacy impacts of changes to the organisation's business practices
- advise their organisation if improving privacy practices might improve the business
- be familiar with any other legislation governing what the organisation can and cannot do with personal information.

Anxiety NZ managers and leaders are responsible for fostering a culture of respect for personal and health information within Anxiety NZ and their teams. Managers are both individually and collectively accountable for:

- Ensuring their teams understand and comply with our privacy policies and procedures

- Actively identifying privacy risks and ensuring all privacy incidents are investigated, reported and resolved in a timely and professional manner.

Anxiety NZ's staff and volunteer workers are expected to consistently demonstrate Anxiety NZ's culture through their behaviour, compliance with our privacy policy and procedures, identification of privacy risks, and by reporting all privacy incidents immediately to their team leader or manager.

Approvals

Document owner - Anxiety New Zealand Trust.

Current version approved by CEO on 7th January 2021.

Next review date 12th January 2021.

The CEO reserves the right to review this policy at any time, which may include in consultation with the Board of Trustees and subject to an approval process.