NZALS
New Zealand Artificial Limb Service
Peke Waihanga, Aotearoa

Data Protection Policy

Table of Contents

1 Background

1.1 NZALS is required by law to have reasonable security mechanisms in place to ensure the data it holds is secure against: loss; access, use, modification, or disclosure except for lawful purposes; or any other misuse.

2 Purpose

2.1 The Data Protection Policy provides guidance on how NZALS and its employees, contractors and Board members will comply with the requirements set out in the Privacy Act, Health Information Privacy Code, Public Records Act and other legal requirements, relating to the management of data held by NZALS. This includes:

a) Health information held about patients, personal information held about employees, and information of suppliers and other organisations held by NZALS; and

b) Data held in any form including, paper, electronic, text or other forms.

3 Scope

3.1 This Policy applies to all NZALS employees, independent contractors, volunteers and Board members.

4 Policy

4.1 NZALS holds personal data relating to employees, patients, suppliers, and other organisations in order to manufacture artificial limbs and provide health services. NZALS is extremely concerned with protecting privacy and confidentiality. NZALS understands that not only employees, but also patients, suppliers and others with whom NZALS comes into contact need to be assured that their data will not be used for any improper purpose, and will not fall into the hands of a third party that has no right or authority to that information. This Policy is relevant to all aspects of data protection, including when data is given to another person or organisation in connection with the provision of services and when any information held by NZALS is disposed of.

4.2 Data protection is the responsibility of all employees, contractors, and Board members. Board members have a particular obligation of confidence in relation to information held in their capacity as a Board member set out in s57 of the Crown Entities Act.

4.3 It is very easy to inadvertently disclose information about a colleague or a patient to other persons including, other patients, friends, or family members. Unless there is a lawful reason for doing so, such a disclosure is a breach of this Policy and of an employee's obligations to NZALS. To avoid this, employees should avoid discussing any aspect of their work with NZALS outside of NZALS that could result in an individual being identified and by doing so breach the individual's privacy.

4.4 NZALS will only share, or disclose personal or health information to a third party, when authorised or required by law, including under NZALS' agreements with funders. All requests for statistical data are to be directed to the Privacy and Complaints Officer or Chief Executive.

4.5 Any action in breach of this Policy may be deemed to be in breach of an employee's employment agreement and could be subject to disciplinary action.

5 Definitions

5.1 **Employee** – For the context of this policy 'employee' includes employees, independent contractors, and Board members.

5.2 **Health information** – Under the Health Information Privacy Code health information includes all information about an identifiable individual that is collected before or in the course of, and incidental to, the provision of any health or disability service to that individual.[1]

5.3 **Personal information** - Under the Privacy Act personal information means any information held about an identifiable person.

6 Data security

6.1 Employee information is kept on NZALS' main server. Access to employee data is protected and is limited to specified employees. If it is necessary to extract any such data for use by another employee, the Privacy and Complaints Officer will ensure the data is only used for the purpose for which it was provided and will ensure that the data has been securely deleted after use.

6.2 All spreadsheets & files with employee information are held in folders which restrict access and files are password protected. Folders with the information are only accessible by persons with either administrator access to the servers or to administration personnel authorised to access company personnel records.

6.3 The payroll system is password protected and the CEO, CFO, Accountant, HR Manager and Finance & Payroll Administrator have a unique password to access the system.

[1] For a full definition of health information under the Health Information Privacy Code refer to clause 4(1) of the Code.

6.4 Employee data is kept for as long as the person is employed by NZALS then is archived for at least seven years from their last date of employment (reference Archives NZ GDA6 – section 3.0.0 Human Resources Management). After this time it is then deleted/securely destroyed in line with NZALS' obligations under the Public Records Act, and Privacy Act.

6.5 Employee data will not be given to any third parties without written permission from the employee unless the information sharing is:

a) Expressly permitted or required by legislation;

b) Permitted by an exception in the Privacy Act (see s6 principles 10 and 11);

c) Permitted by an 'Approved Information Sharing Agreement' under Part 9A of the Privacy Act.

6.6 NZALS has a backup procedure for all data held electronically. Employees involved in any element of backing up data must comply with the backup procedures in a timely manner.

7 Employee Information

7.1 Personal information about employees is collected and held by NZALS to maintain proper employment records in order to comply with legislative requirements and for NZALS' own lawful use. This includes information required for: salary records, leave entitlements and to pay employees, tax purposes, health and safety purposes, and to meet other legal obligations relating to the employee's employment.

7.2 Below is a list of information commonly held by NZALS. NZALS requires the following information to be held on an employee's personnel file. The list is not exhaustive, and other information may also be held:

(a) Letter of appointment;

a) Job description;

b) Employment agreement (individual, if collective employment agreement, copy of front page is sufficient);

c) Personal details including emergency contact, bank details; completed induction forms,

d) Salary related documents addressed to employees i.e. salary reviews or IRD PAYE, Kiwi Saver, Superannuation, deductions for PSA or other;

e) Employment amendments/variations including change in working hours, salary reviews, updated employment agreements;

f) Terms and conditions of employment, including signed Code of Conduct, Email & Internet Usage Policy and induction guide;

g) CV & cover letter;

h) Personal development documentation i.e. Appraisals;

i) Performance Management – meeting notes and/or warnings;

j) Misconduct warnings (be aware of time limits for some warnings);

k) Leave documentation including parental, bereavement etc;

l) Driver's licence if role requires it;

m) Immigration – copies of work permits, residency permits, and if granted citizenship certificate;

n) Workplace Health & Safety related i.e. Accident forms for ACC;

o) Specific correspondence from employee with appropriate responses from NZALS.

7.3 Below are examples of information that should not normally be placed in the employee's personnel file:

a) General day to day emails correspondence about the employee i.e. between Regional Manager and CEO or CFO. Exceptions will apply e.g. management of extended absences due to injury or sickness;

b) Feedback from other employees unless part of a formal performance appraisal;

c) Documentation to National Office about employee e.g. for salary increase request or in reports;

d) Investigation documentation into allegations of misconduct after investigation completed. This information is removed to National Office files only;

e) Employee documentation that includes other employees' information e.g. emails to payroll re employees' changes to pay or leave;

f) Other employees' documentation.

8 Patient information (health information)

8.1 All information about patients collected and held by NZALS while providing services to the patient, including, information required for prescriptions, manufacture, fitting and rehabilitation services, is **health information under the Health Information Privacy Code.**

8.2 Contributing to patient rehabilitation involves working with other health service providers and funders. As part of our normal activities sharing of patients' health information happens on a regular basis. This includes but is not limited to:

a) ACC New limb assessments
b) ACC Replacement limb assessment
c) ACC Repair assessments
d) ACC Rehabilitation plans
e) Referral letters
f) Correspondence with case manager or other health service providers

8.3 Information which does not identify any individual may be used in a general way by NZALS, to provide statistical data. All requests for data not already published on our website will need to be approved by the Privacy and Complaints Officer or Chief Executive Officer.

Handling of health information

8.4 All physical patient documentation including clinical notes, correspondence, referrals, measure charts, rehabilitation plans and funder assessments are kept under the patient's name in locked filing cabinets. The keys to these cabinets are kept by the Regional Manager and are accessible by the Services Coordinator.

8.5 All electronic patient documentation is to be held under the patient's name in Manaaki document manager.

8.6 Information about an identifiable patient must not be left lying around unattended, especially in publicly accessible areas such as reception, and must be stored in the locked filing cabinet when not being used (e.g. no patient information should be left on a desk overnight).

8.7 Privacy breaches represent a significant risk to our stakeholders and the reputation of NZALS. To limit the possibility of a privacy breach relating to use of email the following rules are to be applied at all times:

a) Except for internal emails, only one patient is to be referenced on an email communication;

b) When attaching a document/s the document/s should be opened and checked to ensure it/they contain the intended information before the email is sent;

c) Only the information necessary should be included in an email;

d) When sending an email containing health information the sender should double check the name on the email and should enter the relevant recipient address at the end just prior to sending the email.

e) Exception: NZALS can email multiple patient details in a single email for the purpose of running and facilitating efficient regional clinics with the patient details limited to name, phone number and appointment time.

8.8 When sending information outside of NZALS by email, special care must be taken before sending an entire email thread, especially when the thread has become quite large and contains a mix of personal or health information and general information. When sending health information by email to funders and other health service providers a new email should be started where practicable and the relevant information inserted into it.

8.9 Sending documents by email or courier are now the only accepted methods of sharing an identifiable patient's health information with service providers and funders. Use of fax is no longer acceptable.

8.10 In general, patient information should not be kept on a USB key or portable hard drive unless it has been encrypted, or as otherwise agreed by the Privacy and Complaints Officer (see 6.1). Where patient information (for instance an x-ray image), is brought into a clinic on a USB or other portable device, by a patient or health practitioner, for viewing at a NZALS centre, the USB or other portable device may only be viewed on a Smart TV.

9 Board members statutory obligation of confidence

9.1 Under s57 of the Crown Entities Act a NZALS Board member who has information in his or her capacity as a member that would not otherwise be available to him or her must not disclose that information to any person, or make use of, or act on, that information, 'except'

a) When performing a function for NZALS; or

b) As required or permitted by law; or

c) In accordance with paragraph 9.2 below: or

d) In complying with the requirements for members to disclose interests.

9.2 A member may disclose, make use of, or act on the information if:

a) The member is first authorised to do so by the Board; and

b) The disclosure, use, or act in question will not, or will be unlikely to, prejudice NZALS.

10 Security of hardware/network at work

10.1 It is vital that all hardware used by NZALS or employees for work e.g. all mobile phones, desktop computers, tablet computers, laptop computers, thin clients and iPads are used correctly and securely.

10.2 If any hardware in an employee's possession is lost or stolen it **must** be reported immediately to the Privacy and Complaints Officer and Regional Manager.

10.3 All hardware has an asset number and is registered under the employee's name as the user and the employee is responsible for it while employed with NZALS.

10.4 All NZALS mobile phones, desktop computers, tablet computers, laptops and iPads **must** be either pin protected or password protected.

10.5 Any identifiable patient information held on any mobile device must be removed from the mobile device as soon as it is no longer required to be held on that device.

10.6 Personal mobile devices including mobile phones, tablet computers, laptops and iPads must not be used to obtain or retain identifiable patient information. No identifiable patient data is to be kept on any personal mobile phones, tablet computers, laptops and iPads. Where NZALS mobile devices are used they should be connected to the NZALS servers where the information on the device will be held.

10.7 Employees must ensure their system password is complex with a minimum of 10 characters. This must be made up of at least six letters (one capital), and either four numbers or symbols like %@$.

10.8 Employees must not disclose their password to anybody, the only exception being shared user accounts. These passwords must not be shared outside of NZALS. Passwords must be changed every 90 days. The centre IT delegate will be responsible for changing the shared user account password. If an employee has any suspicion that their password has been compromised for any reason they must change it immediately and inform their centre IT delegate or IT support team.

10.9 NZALS has a very good spam filtering system but like everything some things may get through. Employees must not open any email that looks like it is spam, and if unsure you must check with the IT support team.

10.10 If an employee is using the internet and believes that a file has been inadvertently downloaded on your computer you must report this to the centre IT delegate immediately.

10.11 All NZALS computers run operating system and antivirus updates. Employees must allow the operating system and antivirus system updates to run on their computer or devices. These updates often contain important security fixes and must be allowed to be applied to all NZALS hardware.

10.12 Under no circumstances may hardware provided to an employee by NZALS be used by other person (this includes dependents).

10.13 When the hardware becomes 'end of life' employees must return it to the IT support team so that it can be cleaned/erased. If an employee wishes to purchase the equipment, this can only happen after the hardware has been wiped and has gone through the established open bid process.

10.14 No forms of online shared drives shall be used to transfer files, this includes Dropbox and SkyDrive – under no circumstances are employees to use personal online drives. If an online drive is required in order to transfer files then prior permission needs to be sought from the Privacy and Complaints Officer. The exception to this is marketing information that does not include identifiable patient data, unless the patient has consented to their data or image being used for these purposes.

11 Security of hardware/data working from home

11.1 Sometimes employees may be required to work from home. It is just as important (perhaps even more so) that the Data Protection Policy is followed when working remotely.

11.2 As per paragraph 10.6 of this Policy, no patient data is to be kept on any home devices. Home devices are only to be used to access the NZALS servers via VPN. No identifiable patient data is allowed to be transferred onto these devices.

11.3 If for any reason an employee needs to take an NZALS file home to work on the employee is responsible for registering this with the Privacy and Complaints Officer. If necessary a laptop will be provided to the employee in preference to the employee undertaking NZALS work on a home machine. If it is necessary for any printed material containing personal or health information to be taken home, the employee must ensure this is registered with the Privacy and Complaints Officer and that the employee advises the Privacy and Complaints Officer when the information has been returned. Where possible, in preference to taking printed personal or health information home, any material should be scanned and accessed remotely.

11.4 If an employee uses their home computer to log into NZALS system remotely, and the employee's home computer is used by dependents/partners/flatmates etc. the employee must ensure that he/she logs out of the remote session correctly so it cannot be accessed if the employee walks away from the machine.

11.5 It is NZALS policy that employees **must not** allow the system to remember their password. Employees must always type in their user name and password, and not allow the system to remember it.

11.6 All home wireless units must be secured with encryption enabled and password to authenticate users.

11.7 If an employee is not able to provide antivirus for their home machine they must advise the IT support team who will provide the employee with a licence (for as long as the employee is employed by NZALS)

12 Financial information, including credit card details

12.1 Financial and credit card information is used to obtain payment for goods and services ordered from NZALS. NZALS does not use the information obtained for payment for goods and services for any other purpose unless legally permitted or required to do so. NZALS only holds this information for as long as it is required to process a payment or to meet any other legal requirements, including under the Public Records Act.

13 Supplier information

13.1 Suppliers provide NZALS with their information in the course of doing business with NZALS. This information is used by NZALS to maintain its accounts, business and job costing records.

13.2 NZALS employees must protect supplier's confidential or commercially sensitive information. This includes information that could compromise fair competition between suppliers. A supplier's confidential or commercially sensitive information will only be disclosed if:

a) The supplier has already agreed to the disclosure in writing (email is fine); or

b) The disclosure is permitted or required by law (e.g. under the Official Information Act, or any other Act or Regulation); or

c) It is a limited disclosure expressly notified in a Notice of Procurement which suppliers have consented to by participating in the process.

13.3 When responding to a supplier's questions, employees must take care not to discuss or disclose another supplier's confidential or commercially sensitive information.

14 Disclosure to Government agencies

14.1 NZALS will only disclose personal or health information, or information that is commercially sensitive, if permitted or required under the Privacy Act, Health Information Privacy Code, Health Act or any other law. The Privacy and Complaints Officer must be notified of any request for information by a government agency or the police.

15 Information request by an employee

15.1 At any time employees may ask to review or update the personal information that NZALS holds about them. If the request relates to pay, leave, or other day-to-day employment matters the request should be forwarded to the Finance & Payroll Administrator. Any other request, or a request to correct information held about the employee should be treated as a request under Principle 6 or 7 of the Privacy Act and all such requests must be forwarded to the Privacy and Complaints Officer.

16 Managing a data breach

16.1 The Privacy and Complaints Officer is responsible for managing the response to all data or privacy breaches. Any data or privacy breach is considered a serious matter. A data or privacy breach is the result of unauthorised access to or collection, use or disclosure of personal information. All privacy breaches (actual or potential) must be reported to the Privacy and Complaints Officer without delay. Refer to the Privacy Policy for further information on managing data or privacy breaches.

17 Specific responsibilities

Party	Responsibilities
All employees	• Ensuring knowledge and understanding of their obligations under this Policy. • Reporting lost or stolen NZALS devices in their possession. • Immediately notifying IT that their device is compromised e.g. virus, Trojan etc.
Regional Managers/Team Leader	• Ensuring appropriate security of physical records containing personal or health information. • Disposal of records, in conjunction with the Privacy and Complaints Officer, in compliance with the Public Records Act when no longer required to be held by NZALS. • Ensuring employees are trained in and aware of their obligations under this Policy.
IT Delegates	• Maintaining passwords for shared user accounts.
IT Support team	• Password reset, responding to reports of suspicious content, wiping of hardware devices at end of life.
Privacy and Complaints Officer	• Authorising release of statistical data, extraction of data for specific purposes. • Granting permission for transfer of data to USB or portable hard drive. • Maintaining register for physical files removed from premises for working from home. • Coordinating response to requests for disclosure of personal or health information, or commercially sensitive information. • Coordinating NZALS' response to any data breach.
CEO	• Ensure NZALS complies with its legal obligations in relation to data security, has a fit for purpose Data Protection Policy, and employees are aware of their obligations under the Policy. • Reporting any data or privacy breaches to the Board, and determining whether the Office of the Privacy Commissioner should be notified. • Authorising release of statistical data approved by the Privacy and Complaints Officer
Board	• Endorsing this Policy. • Individual Board members must comply with members' obligations under this Policy and s57 of the Crown Entities Act.

18 Legal compliance

- Official Information Act 1982
- Crown Entities Act 2004
- Health Act 1956
- Health Information Privacy Code 1994
- Health (Retention of Information) Regulations 1996
- Privacy Act 1993
- Public Records Act 2005
- New Zealand Government Procurement Reform Programme (GPRP)

19 Related Policies, Procedures and Forms

- Privacy Policy
- Privacy Statement & Privacy Consent Form
- Internet & Email Use Policy
- Code of Conduct Policy
- Discipline Policy
- Mobile Device Usage Policy
- Communications Policy
- *Records Management Policy (in production)*
- *Transfer & Disposal Destruction procedure (in production)*

20 Revision History

Author	Version number	Version date	Description of changes
Compliance Advisor	3.4	July 2017	Amendments from Data Controller to Privacy and Complaints Officer, add CFO & Regional Manager. Updates to use of Fax and retention period for archiving employee data
Claro Law	3.3	April 2016	Changes to handling of health information
CEO	3.2	February 2016	Email exception for regional clinic
CEO	3.1	December 2015	Incorporation of feedback from Claro and updated branding
Compliance Advisor	2.2	June 2015	Addition of an personal copy of the acknowledgment page

Placeholder page only

NZALS
New Zealand Artificial Limb Service
Peke Waihanga, Aotearoa

Data Protection Policy (Personal copy)

I have read and understood the **NZALS Data Protection Policy** and agree to abide by this Policy. Please retain this copy for your own records.

_____

Name

_____ _____

Signed Date

Placeholder page only

NZALS
New Zealand Artificial Limb Service
Peke Waihanga, Aotearoa

Data Protection Policy (File copy)

I have read and understood the **NZALS Data Protection Policy** and agree to abide by this Policy. Please return this signed page to your Manager.

_____

Name

_____ _____

Signed Date