

# Privacy Policy

## Table of Contents

1	Background .....	2
2	Purpose .....	3
3	Scope .....	3
4	Policy .....	3
5	Definitions .....	5
6	Collection of information (Rules 1-4, Principles 1- 4) .....	6
7	Storage and security of information (Rule 5, Principle 5) .....	10
8	Access to information by the person concerned (Rule 6, Principle 6).....	11
9	Requests for correction of information (Rule 7, Principle 7) .....	13
10	Accuracy of information (Rule 8, Principle 8) .....	14
11	Retention of information (Rule 9, Principle 9) .....	14
12	Using information (Rule 10, Principle 10) .....	15
13	Disclosing information (Rule 11, Principle 11) .....	16
14	Managing a data or privacy breach or complaint.....	29
15	Specific responsibilities .....	30
16	Legal compliance .....	31
17	Related Policies, Procedures and Forms .....	31
18	Revision History .....	32

## 1 Background

- 1.1 The Privacy Act 1993 ('Privacy Act') is New Zealand's main privacy law relating to persons, and provides a framework for regulating the collection, storage, use, and disclosure of personal information.
- 1.2 The Health Information Privacy Code ('HIPC'), a regulation under the Privacy Act, regulates how individuals and organisations must deal with health information. The rules in the HIPC replace the information privacy principles in the Privacy Act with more specific privacy principles in relation to health information. All other provisions in the Privacy Act apply to health information in the same way as personal information. In addition, many other statutes also include specific provisions that may require or authorise NZALS to collect or provide information.
- 1.3 NZALS is a public sector organisation and is also subject to the Official Information Act 1982 ('OIA'), and the Public Records Act 2005. The primary principle of the OIA is that official information held by government and government agencies and departments (including NZALS) should be made available unless there is good reason for withholding it. Further information on the NZALS' legal obligations under the OIA is found in the **Official Information Policy**. Information about requirements under the Public Records Act 2005 is found in the **Data Protection Policy**.
- 1.4 Health professionals' regulatory authorities and professional bodies have specific guidelines and/or statements in their Codes of Ethics covering confidentiality of patients' health information. Health professionals should be familiar with, and comply with, statements and guidelines implemented by their regulatory authority and professional bodies.
- 1.5 The rights and obligations in the Code of Health and Disability Services Consumers' Rights ('HDC Code of Rights') may also be relevant to how a patient's information may be collected and used. The following rights are particularly relevant: Right 1(2) - right to privacy, Right 4(5) – right to cooperation between providers, Rights 6 and 7 – right to information and to make an informed decision, and Right 9 – rights to be told if they are participating in teaching or research.
- 1.6 The Privacy Act, HIPC, other statutes, and standards and guidelines from professional bodies and regulatory authorities may be used by the Privacy Commissioner, the Health and Disability Commissioner, the Coroner, Human Rights Review Tribunal, and Health Practitioner's Disciplinary Tribunal as identifying the legal obligations and relevant standards by which an organisation, health professionals, and other employees' conduct is measured.

## 2 Purpose

- 2.1 The purpose of this Policy is to set out key principles and procedures NZALS and its employees should use to ensure the organisation and employees meet their legal obligations in relation to managing, using and disclosing personal and health information.

## 3 Scope

- 3.1 This Policy applies to all information held by NZALS, including personal information about employees and health information about patients and applies to all NZALS employees and Board members, and any other person or organisation dealing with personal or health information on behalf of NZALS. This includes volunteers, students and contractors.

## 4 Policy

- 4.1 This Policy:
- (a) establishes the framework for managing information and protecting individual's privacy;
  - (b) sets out obligations and responsibilities that NZALS and employees must meet in order to comply with key legal obligations in the Privacy Act, HIPC, and other relevant legislation in relation to personal and health information held by NZALS;
  - (c) sets out NZALS' requirements when investigating and managing an actual or potential privacy breach.
- 4.2 This Policy must be read in conjunction with the following NZALS policies and statements:
- (a) **Privacy Statement and Privacy Consent Form** – The NZALS Privacy Statement summarises how NZALS collects, stores, uses and disclosed patient's health information. A copy of the Privacy Statement must be given to, and be explained to each patient when they first become a patient of NZALS. The signed Privacy Consent Form must be filed in the patient's record.
  - (b) **Data Protection Policy** - sets out in greater detail NZALS' requirements and employees' obligations in relation to storage and security of information; and
  - (c) **Records Management Policy** - sets out NZALS' obligations in relation to management of information under the Public Records Act 2005;
  - (d) **Complaints Policy** – applies to the management of all complaints received by NZALS including complaints relating to how a person's information has been collected, stored, used and disclosed;

- (e) **Mobile Device Usage Policy** – sets out the standards, procedures and restrictions on the use of personal mobile devices for work related purposes;
- (f) **Internet and Email Use Policy** – which sets out employees’ responsibilities and obligations when using internet or email;
- (g) **Official Information Policy** – sets out NZALS’ obligations under the OIA.

4.3 This Policy, the Privacy Act and HIPC are technology neutral and apply with respect to information no matter what form the information is held in.

4.4 The key principles that should guide decision-making when considering whether to collect, use or disclose health or personal information can be summarised as:

- (a) **Compliance with the core legal obligations:** Employees must be aware of, and comply with, their core legal obligations relating to the collection, use, storage and disclosure of health and personal information.
- (b) **Openness and honesty:** When collecting information employees should be open and honest about the purpose for which the information will be used, and what information will be shared with whom. In general there should be a ‘no surprises’ approach.
- (c) **Information should be used and disclosed with the person’s consent where appropriate and where practicable:** In most cases the wishes of the person whose privacy interest is at stake should be respected. Information may be used and disclosed in limited circumstances without consent, as set out in the Privacy Act, HIPC and statutes which allow disclosure without consent (for more information refer to section on disclosure in this Policy). Whether to disclose or not, where disclosure is permitted by law, will be a matter of professional judgement. Key considerations include:
  - i. **Always consider safety and wellbeing:** The safety of the person concerned and other persons who may be affected by the person’s actions must be a paramount consideration when exercising discretion to disclose in the absence of express consent.
  - ii. **Disclosure must be necessary, proportionate, relevant, accurate, timely, and secure:** Only information necessary for the purpose for which the disclosure is made should be disclosed, and only to those persons who need to know or who can do something to mitigate or minimise any risk or harm. The information must be accurate, and up-to-date, and be disclosed in a secure and timely manner.
  - iii. **Keep a record:** Where information is used or disclosed in a manner that was not anticipated at the time of collection, this must be recorded.
  - iv. **Seek advice:** Advice should be sought from a senior colleague, NZALS’ Privacy and Complaints Officer, or NZALS’ lawyer in complex or difficult situations to ensure information is being disclosed legally and professionally.

## 5 Definitions

- 5.1 **Employee** – means all NZALS current and former employees, Board members, persons providing services under contract to NZALS, volunteers, students and any other person involved in NZALS operations.
- 5.2 **Health practitioner** – the term ‘health practitioner’ in the HIPC refers to health professionals who are registered under the Health Practitioners Competence Assurance Act 2003 (‘HPCA Act’). Health professionals who are not registered under the HPCA Act are not ‘health practitioners’ for the purposes of the HIP Code or this Policy. They are a ‘health agency’ under the HIPC and are subject to the obligations under the HIPC. ‘Health practitioners’ have some additional rights to disclose information under Rule 11(2) that do not apply to other health professionals.
- 5.3 **Health information** is defined in the HIPC to mean:
- (a) information about the health of an individual, including his or her medical history; or
  - (b) information about any disabilities an individual has, or has had; or
  - (c) information about any health services or disability services that are being provided, or have been provided, to an individual; or
  - (d) information provided by an 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
  - (e) information about an individual which is collected before or in the course of, and incidental to, the provision of any health service or disability service to that individual.
- Note: The definition of health information under the Health Act does NOT include (e) above.
- 5.4 **Information** - includes personal information and health information. Information is not confined to what is written but includes any knowledge gained or held. Information may be contained for instance in written notes, emails, audio, CCTV recordings, and photos.
- 5.5 **Personal information** - is information about an identifiable individual.

5.6 **Representative**, in relation to an individual, is defined in the HIPC and Health Act to mean:

- (a) where that individual is dead, that individual's personal representative; or
- (b) where the individual is under the age of 16 years, that individual's parent or guardian; or
- (c) where the individual, not being an individual referred to in paragraphs (a) or (b), is unable to give his or her consent or authority, or exercise his or her rights, a person appearing to be lawfully acting on the individual's behalf or in his or her interests (e.g. a welfare guardian or Enduring Power of Attorney).

5.7 **Working day** – is defined in the Privacy Act and OIA to mean 'any day of the week other than:

- (a) Saturday, Sunday, Good Friday, Easter Monday, Anzac Day, Labour Day, the Sovereign's birthday, and Waitangi Day; and
- (b) if Waitangi Day or Anzac Day falls on a Saturday or a Sunday, the following Monday; and
- (c) a day in the period commencing with 25 December in any year and ending with 15 January in the following year.'

Note: The working day count for responding to an official information request: starts the day after a request is 'received'. A calculator that works out the 20 working day limit is available at <http://www.ombudsman.parliament.nz/>.

## 6 Collection of information (Rules 1-4, Principles 1- 4)

### Collecting health or personal information (Rule 1 & 3, Principle 1 & 3)

6.1 Strict rules apply to the information NZALS may collect about employees and patients.

6.2 NZALS must only collect information for a **lawful purpose**. The information:

- (a) must be connected with a **function or activity** of NZALS; and
- (b) must be **necessary** for that purpose.

6.3 What is 'lawful' to collect will depend on the circumstances. As an example it would not normally be necessary (or lawful) for NZALS to ask another provider for a patient's 'entire history' or 'complete medical file.'

6.4 **The purpose(s) for which information is collected and may be used or disclosed is very important.** NZALS must take reasonable steps to make sure the person concerned knows:

- (a) what information is being collected;
- (b) the purpose for which the information is collected;
- (c) who the information may be shared with and who will see the information;
- (d) what will happen if the information is not provided.

As long as at the time of collection the person is made aware of the purpose(s) for which their information is collected and may be used or disclosed, the information can be used for these purposes without seeking authorisation from the person.

6.5 The general purposes for which NZALS collects information, and information regarding how information is secured, used and may be disclosed by NZALS is set out in the **NZALS Privacy Statement.**

6.6 **A copy of the Privacy Statement must be given to, and be explained to each patient when they first become a patient of NZALS. The signed Privacy Consent Form must be filed in the patient's record.**

6.7 It is not necessary to repeat this information, or obtain consent from the patient each time a patient receives services, provided the information and purpose for which the patient's information will be used remain the same.

6.8 If the information is being collected for a purpose that is outside the purposes set out in the Privacy Statement this must be explained to the patient.

6.9 The HIPC provides for exceptions to this Rule when collecting health information if:

- (a) doing so would undermine the purpose for which the information is collected or prejudice the interests of the person concerned (Rule 3(4)(b)); or
- (b) it is not reasonably practicable in the circumstances to tell the person (Rule 3(4)(c)); or
- (c) to do so would prejudice a public sector body upholding or enforcing the law (Rule 3(4)(d))

6.10 When collecting personal information that is not health information the exceptions in Principle 3 of the Privacy Act will apply in place of the exceptions in Rule 3 of the HIPC. The exceptions in the Privacy Act are similar to, but different from the exceptions in Rule 3 of the HIPC.

## Source of information (Rule 2, Principle 2)

- 6.11 Where possible information must be collected from the person concerned.
- 6.12 Rule 2 of the HIPC or Principle 2 of the Privacy Act set out the limited circumstances when information may be collected from a person other than the person concerned.
- 6.13 In relation to health information, the exceptions in Rule 2 that are most likely to apply to NZALS include for example:
- (a) when the patient has **authorised** collection from someone else (e.g. a family member or friend). The person should clearly understand who they are allowing to give **what** information (Rule 2(2)(a)). Where practicable the person's authorisation should be obtained in writing and should be recorded on their file.
  - (b) if collecting information directly from the patient would prejudice their interests; or the purpose of collection (such as treatment), or it may prejudice the safety of another person (Rule 2(2)(c));
  - (c) if the patient cannot be found or contacted, or does not know the information sought (Rule 2(2)(d));
  - (d) where the information is collected from a publicly available source (Rule 2(2)(f));
  - (e) if the information collected will not be used in a form in which the person concerned is identified; or will be used for statistical purposes, or research purposes (for which approval by an ethics committee, if required, has been given), and will not be published in a form that could reasonably be expected to identify the person concerned (Rule 2(2)(g));
  - (f) it is necessary for a public sector agency to uphold or enforce the law (Rule 2(2)(h)(i)); or
  - (g) in certain circumstances where it is necessary for the purposes of court or tribunal proceedings (Rule 2(2)(h)(iii))

Note: All information collected in relation to a patient will come within the definition of health information and collection will be governed by Rules 1 – 4 of the HIPC. If personal information, not associated with a patient is collected (for instance about an employee), the exceptions in Principle 2 of the Privacy Act (not Rule 2) will apply.

- 6.14 Where information has been collected from someone other than the person concerned, it is good practice to check the accuracy of the information collected with the person concerned before it is used, where this is practicable and appropriate.

## Unsolicited information

- 6.15 Information may be received by NZALS that it has not asked for or sought in any way (e.g. information provided by a relative or any other person of their own volition). In this case Rules/Principles 1- 4 will not apply. However, if NZALS keeps the information it must comply with the other Rules/Principles in the HIPC or Privacy Act. How the information was obtained should be clearly recorded in the person's file.

- 6.16 If NZALS wants to use or disclose unsolicited information it is good practice to check the accuracy of the information with the person, where this is practicable and appropriate. This is particularly so if the information relates to a patient and will be used for treatment or providing services or any other action.
- 6.17 It may not be possible, or appropriate to keep the information itself or the identity of the person who provided the information secret. For this reason a promise of confidentiality should not be given when receiving unsolicited information.

#### Collection from other health or disability service providers

- 6.18 NZALS may **request relevant information** about a patient it is, or is to, provide services to under section 22F of the Health Act. Only information necessary for NZALS to provide the service(s) should be requested.
- 6.19 It is not a requirement under section 22F of the Health Act to obtain the consent of the person concerned, and if the patient has been given a copy of the **NZALS Privacy Statement** and has signed the **Privacy Consent Form** in most circumstances this would be sufficient. However, if NZALS is aware that the patient would be likely to object to NZALS obtaining any information from another provider the Privacy and Complaints Officer should be consulted before proceeding. In this situation it would in most cases be good practice to inform the patient NZALS wants to obtain the relevant information from the other provider before proceeding. Any objection to this from the patient should be carefully considered before deciding whether to proceed with the request.
- 6.20 In all instances where a request is made for information under section 22F of the Health Act the request and any discussion with the patient must be recorded in the patient's Manaaki notes.

#### Manner information is collected (Rule 4, Principle 4)

- 6.21 NZALS must only collect information by **lawful means that are not** in the circumstances **unfair or unreasonably intrusive**. In most situations for instance it would not be fair or reasonable to secretly record a meeting with a person without their knowledge.
- 6.22 When collecting information of a sensitive or confidential nature NZALS will ensure that the person concerned has physical privacy in which to provide the information, where this is possible (Refer to Right 1(2) of the HDC Code of Rights).
- 6.23 Any questions or concerns about the lawfulness of the manner in which information is to be collected should be referred to the Privacy and Complaints Officer.

#### Clinical photographs and recordings

- 6.24 The collection, use, storage, retention, and disclosure of photographs and recordings about an identifiable patient are governed by the HIPC, in the same way as all other health information. When collecting and/or sharing photographs or recordings, as with collecting all other information; there are legal, professional, and ethical responsibilities that must be complied with.

- 6.25 A photograph or recording must only be taken for appropriate purposes which the patient has been informed of, and agrees to, and must:
- (a) only be used for the purpose it was obtained for or a directly related purpose;
  - (b) only be used for another purpose if the patient consents to the use, or the use is permitted by the HIPC, or any other statutory provision;
  - (c) be stored securely against unauthorised access or use (e.g. encrypted if kept on a USB stick, files stored securely i.e. in a locked cabinet).
- 6.26 NZALS does not permit patient photography or recordings to be taken on personal devices, including smart phones. Please refer to **Personal Mobile Device Use Policy**.
- 6.27 If a photograph or recording is to be used for anything other than clinical care and maintaining a record in the clinical record the patient must have given explicit consent for the additional use. This includes uses such as training and education, publication, promotion, and research. The patient's consent must be recorded in the clinical record.
- 6.28 If a photograph or recording is to be used for education or research the photograph or recording should be de-identified where possible and must comply with relevant research or ethical guidelines.

## 7 Storage and security of information (Rule 5, Principle 5)

- 7.1 NZALS takes the security of the information it holds about patients and employees seriously, and ensures reasonable security safeguards are in place to protect against:
- (a) Loss;
  - (b) Unauthorised access, use, modification or disclosure; and
  - (c) Other misuse
- 7.2 NZALS is responsible for the information it holds and information it provides to any person or organisation acting on its behalf. Where NZALS provides information (or access to information) to a third party in connection with providing services to the patient, NZALS will ensure a non-disclosure or confidentiality agreement is signed to prevent unauthorised use or disclosure of information by that person or organisation.
- 7.3 The **Data Protection Policy** sets out NZALS' requirements and obligations in relation to ensuring the physical, electronic, and operational security of information held by NZALS or its agents. The Data Protection Policy applies to both patient and employee information and establishes NZALS' requirements for:
- (a) how NZALS will ensure the security of the information it holds;
  - (b) NZALS procedures for safely storing and managing information held by NZALS;
  - (c) the use of NZALS confidential information.
- 7.4 All employees are required to be aware of and comply with the **Data Protection Policy**.

- 7.5 Health information is generally considered inherently sensitive. Patient information may only be accessed by employees in the course of providing services to the patient or as otherwise authorised. Unauthorised access of a patient's health information may be serious misconduct and action may be taken against the person making the unauthorised access under the NZALS **Discipline Policy**.
- 7.6 Employees' also expect their personal information to be kept private and to be held securely. Only persons authorised to access a particular employee's information will have access to that information. NZALS performs regular audits of access to employee information held on its IT system. Any unauthorised access may be serious misconduct and action may be taken against the person making the unauthorised access under NZALS **Discipline Policy**.

## 8 Access to information by the person concerned (Rule 6, Principle 6)

- 8.1 The starting point is that persons have a broad right to access information held about them. Under Rule 6/Principle 6 any person is entitled to:
- (a) know whether NZALS holds information about them; and
  - (b) access information NZALS holds about them that is readily retrievable.
- 8.2 A request 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 Privacy Act or HIPC.
- 8.3 An access request should be forwarded to the Privacy and Complaints Officer in the first instance. The Privacy and Complaints Officer will be responsible for logging the request and ensuring the timeframe and obligations under the Privacy Act or HIPC for responding to the request is met.
- 8.4 When a request is received for health or personal information by the person concerned or their agent there is an obligation on NZALS to:
- (a) **provide assistance to the person** if required (section 38 Privacy Act);
  - (b) **transfer the request to another agency** within 10 working days of receiving the request, and informing the person accordingly, if NZALS does not hold the information or if the information is more closely related to that other agency (i.e. where NZALS has received a copy of a report from another agency) (section 39 Privacy Act and refer to definitions section re how to work out working days);
  - (c) **inform the person of the decision regarding their request** as soon as reasonably practicable and within 20 working days (section 40 Privacy Act);
  - (d) **provide the information that is to be released**. The information does not have to be released at the same time as the person is informed of the decision on the request, although it often will be. If the information is not provided at the same time it must be provided without **undue delay** (section 40 Privacy Act);

- (e) **make the information available in the form requested** by the person unless to do so would: impair the efficient administration of NZALS; be contrary to any legal duty NZALS has in respect of the information; or prejudice the interests protected under sections 27 – 29 of the Privacy Act (section 42 Privacy Act).
- 8.5 **When NZALS informs a person of the decision** in response to an information request, (see para 9.4 (c) above) NZALS must inform the person of their:
- (a) right to have the decision reviewed by the Privacy Commissioner; and
  - (b) right to request correction of any information they believe is incorrect under Rule 7 or Principle 7 respectively.
- 8.6 **If NZALS' decision is to refuse access to some or all of the information requested**, it must tell the requester:
- (a) the reason for the refusal;
  - (b) that they have a right to make a complaint to the Privacy Commissioner and to seek an investigation and review of the refusal; and
  - (c) if the person requests it; the grounds in support of the reason, unless giving those grounds would itself prejudice the interests protected under sections 27 – 29 of the Privacy Act.
- 8.7 **NZALS can only withhold information** following an access request by the person concerned or their agent in limited circumstances set out in sections 27 – 29 of the Privacy Act. The main reasons that may be relevant to NZALS are:
- (a) Providing the information would:
    - i. endanger the safety of any person (section 27(1)(d)); or
    - ii. prejudice the detection and investigation of criminal offences (section 27(1)(c)); or
    - iii. involve the unwarranted disclosure of someone else's affairs (section 29(1)(a)); or
  - (b) The information is:
    - i. evaluative material defined in section 29(3) (section 29(1)(b)); or
    - ii. not readily retrievable/cannot be found/does not exist (section 29(2)).
- 8.8 The right is to access information (which in most cases will be by receiving a copy of that information) but not to demand original documents.
- 8.9 A request cannot be refused on the basis that the person does not 'own' the information.
- 8.10 NZALS cannot charge for making information available following an access request under the Privacy Act or HIPC.

- 8.11 A failure to comply with the obligations under Rule 6 or Principle 6 constitutes an interference with the person's privacy even if the person has not suffered any harm (section 66(2) of the Privacy Act).
- 8.12 A person can appoint an agent to act on their behalf. NZALS must verify that the person requesting the information on another person's behalf actually does have the authority of the person concerned. NZALS should request the authorisation in writing and check the identity of the agent before releasing any information to the agent. This verification must be recorded in the person's file.

## 9 Requests for correction of information (Rule 7, Principle 7)

- 9.1 People have a right to ask for information about them to be corrected if they think the information is wrong. This applies to patients and employees.
- 9.2 If NZALS receives a request to correct information it must inform the person of its decision on the request as soon as reasonably practicable and within 20 working days of receiving the request (section 40 Privacy Act) (Refer to definitions section for calculating 20 working days).
- 9.3 NZALS has an obligation under Rule 8/Principle 8 to ensure information they propose to use is accurate. However, NZALS does not have to make a correction requested if it reasonably believes it is not appropriate to make the correction. Reasons for refusing a request for correction might include that:
- (a) NZALS is satisfied the information is correct;
  - (b) the information is clearly identified as opinion material and correctly represents the opinion held at the time – removing or changing the earlier information would leave a course of action unexplained;
  - (c) the information was believed to be correct at the time, circumstances have changed, and now there is no means of verifying its accuracy.
- 9.4 There is no obligation to hold only factually correct information. For instance reasonably held opinions of the writer at the time the information was compiled can also be included in the record. Making a correction as requested might result in the information being inaccurate and incomplete.
- 9.5 If NZALS agrees there is an inaccuracy in the information, it must correct it. Correction may include altering information by way of correcting, deleting, or adding information.
- 9.6 **If NZALS does not agree to correct the information**, it must give the person the opportunity to add their views by attaching a statement of correction to the information in question.

- 9.7 When steps are taken to correct information or attach a statement from the requestor seeking correction, NZALS must then take reasonable steps to:
- (a) inform everyone who has previously received the information (this could be by way of an email, a telephone call or a letter) of any changes made; and
  - (b) ensure that the statement or correction will be read in conjunction with the disputed information.
- 9.8 If a request for correction is ignored, NZALS does not respond within the timeframes in para 10.2 above, or the request is refused and there is no proper basis for the refusal, under the HIPC and Privacy Act this will amount to an interference with the person's privacy even if the person has not suffered any harm (section 66(2) of the Privacy Act).

## 10 Accuracy of information (Rule 8, Principle 8)

- 10.1 Before using information, NZALS must take reasonable steps to check that the information is up-to-date, complete, relevant and not misleading. What is reasonable will depend on where the information was obtained and when it was obtained. It will also depend on the proposed use of the information.
- 10.2 This is particularly important if the information was obtained from a source other than the person concerned. It may be necessary for instance where health care entitlements or treatment decisions and alternatives are based on the information to check the accuracy of the information with the person concerned.
- 10.3 The information may be in the form of an opinion or comment 'about' the person. It is not necessary that the person concerned agrees that the information that is opinion material is accurate, if the information correctly represents the opinion of the writer and the opinion was reasonably held at the time. What is important is that there were reasonable grounds for believing that the information held was correct at the time it was made.

## 11 Retention of information (Rule 9, Principle 9)

- 11.1 NZALS has legal obligations in regard to the retention of information under the Public Records Act 2005 and the Health (Retention of Health Information) Regulations 1996.
- 11.2 NZALS will meet any legislative requirements for retaining information and will not retain information for longer than is required by law or for the purposes for which it may lawfully be used. When information is no longer required it can be returned, destroyed or transferred in accordance with the requirements in the Public Records Act 2005.

### Obligations under the Health (Retention of Health Information) Regulations 1996

- 11.3 The Health (Retention of Health Information) Regulations 1996 require all health information held by NZALS to be kept for at least ten years from the last date services were provided to the person, unless the information has been transferred to another provider or given to the person.

### Obligations under the Public Records Act 2005

- 11.4 Under the Public Records Act 2005, all public offices, including NZALS are required to create and maintain full and accurate records in accordance with normal, prudent business practice. This applies to all information, including health information, held by NZALS.
- 11.5 NZALS' **Record Management Policy** establishes a framework to ensure that all NZALS information (records) are created, managed and disposed of in a way that meets NZALS' legal obligations under the Public Records Act 2005. For disposal of any records held by NZALS refer to the Record Management Policy.

## 12 Using information (Rule 10, Principle 10)

- 12.1 NZALS will only use information for the purpose(s) that it was obtained, unless an exception in Rule 10 or Principle 10, or another legal authority applies. Health information may also be used for directly related purposes under Rule 10(1)(b) (e.g. information obtained for care and treatment may be used for administrative purposes related to that care and treatment).
- 12.2 Rule 10/Principle 10 sets out limited circumstances when information may be used in a way which was not anticipated when it was obtained. The grounds most likely to apply to NZALS includes when NZALS believes on reasonable grounds:
- (a) **the other use was authorised** by the person or their representative (Rule 10(1)(a)/Principle 10(a)). The authorisation of the patient or their representative must be recorded in the patient's Manaaki file, or in the case of personal information relating to an employee in the employee's HR file; or
  - (b) relevant information may always be used for another purpose where necessary to prevent or lessen a **serious threat** to public health or public safety, or somebody's life or health (Rule 10(1)(d)/Principle 10(d));
  - (c) information may also be used if it is necessary to **avoid prejudice to the maintenance of the law** by a public sector agency (e.g. Police, CYFS), or for the conduct of proceedings before a Court or Tribunal (Rule 10(1)(f)/Principle 10(c));
  - (d) that the information is used in a form in which the person concerned is **not identified**; or is used for **statistical or research purposes** (for which approval by the ethics committee is required, has been given) and will not be published in a form that could reasonably be expected to identify the person concerned (Rule 10(1)(e)/Principle 10(f)).

- 12.3 When considering whether or not information may be used in a way that is not connected to the original purpose it was collected for, the Privacy and Complaints Officer should be consulted for advice and guidance.
- 12.4 Where information has been used in connection with a purpose that is different to the purpose for which the information was collected, the reason for using the information in that way, and the exception to Rule 10/Principle 10 or other legal authority that authorises the use, must be recorded in the person's file (the patient's Manaaki file, or in the case of personal information relating to an employee in the employee HR file).

### 13 Disclosing information (Rule 11, Principle 11)

- 13.1 Disclosing a person's health or personal information can cause special difficulties and become an issue when NZALS:
- (a) **has** to disclose information (the disclosure is required by law);
  - (b) **wants** to disclose information;
  - (c) has been **asked** to disclose information.
- 13.2 Before disclosing information the following key factors should be considered:
- (a) Is there a clear and legitimate purpose for disclosing the information?
  - (b) Is the information identifiable personal or health information?
  - (c) Does the person concerned consent to the disclosure?
  - (d) Is disclosure required by law?
  - (e) Is there discretion to disclose?
  - (f) Is the information disclosed appropriately, proportionately and securely?
  - (g) Has the decision been properly recorded?
- 13.3 These factors are discussed in the sections below.

#### Is there a clear and legitimate purpose for disclosing the information?

- 13.4 The starting point is that an organisation or person who holds an identifiable person's information, **must not disclose the information except in the following situations:**
- (a) if the person concerned **consents** to the disclosure the disclosure can be made;
  - (b) if the disclosure is for a **purpose(s)** the information was obtained and the person was advised of this, before the information was collected, the information can be disclosed for those purposes in accordance with Rules 3, 10 and/or 11 of the HIPC or Principles 3, 10 and/or 11 of the Privacy Act;

(c) **where neither of the above applies another legal basis must be found to allow the disclosure.** This must be either:

- i. **another statute that allows or requires disclosure** of the person's information. A statute that allows or requires the disclosure will override the HIPC or Privacy Act; or
- ii. **an exception in Rule 11 or Principle 11.** If there is no other statute that allows NZALS to provide the information, NZALS **must not disclose the information unless an exception in Rule 11 of the HIPC or Principle 11 of the Privacy Act applies.**

13.5 As part of good clinical practice, a person should normally be included in decisions regarding the use and disclosure of their health or personal information, unless to do so would prejudice the reason for disclosure.

13.6 If the disclosure is not an anticipated purpose or the person has not consented to the disclosure the Privacy and Complaints Officer must be consulted prior to the disclosure of information.

13.7 Note: Unlike the other Rules in the HIPC and Principles in the Privacy Act, Rule 11 and Principle 11 applies to information about a deceased person as well as living persons.

#### **Is the information identifiable personal or health information?**

13.8 Non-identifiable personal or health information can be disclosed. Where ever practicable, information should be anonymised before it is disclosed.

#### **Disclosure with the person's consent**

13.9 **Information can always be disclosed with the person's consent.** Consent may be verbal or written. However, to be valid, consent must be informed and freely given. This means the person:

- (a) must know what information is likely to be disclosed;
- (b) to whom and for what purpose the information will be shared;
- (c) agrees to this without any duress;
- (d) is mentally capable of making the decision

13.10 Consent can also be withdrawn at any time. If a person refuses to authorise disclosure, or withdraws their consent to disclosure he/she should be informed of any possible implications of the decision to withhold their consent to disclosure of their information, particularly to other health providers.

13.11 If a person is unable to exercise their rights under the HIPC or Privacy Act, including not having the mental capacity to give or withhold consent to the disclosure of their information, disclosure can be made to, or with the authority of a representative.

### Is disclosure required by law?

- 13.12 Any law that **requires** information to be made available takes precedence over the HIPC or Privacy Act. If the words ‘**shall**’ or ‘**must**’ are used in relation to disclosure of information in a statute then the disclosure is **mandatory** and the relevant information **must** be made available.
- 13.13 If a particular statute or provision in a statute is cited as authority for a request, the requestor **must** be asked to provide the request in writing, including what statutory provision they are relying on, and the reason for requesting the information (this can be by email). Except in exceptional circumstances, the information should not be disclosed until the actual authority (i.e. the search warrant or Court order, or statutory provision the requestor is relying on) has been sighted. Any disclosure must be confined to the scope of the request and information that comes within the limits set out in the relevant statutory provision.
- 13.14 It is common for an organisation to state that it has statutory authority to demand information when in fact the statute referred to only **allow** the requestor to request the information and provides the person or organisation that holds the information (NZALS) with discretion to release the information.
- 13.15 Even where disclosure is required by law it is in most situations good practice, although not a legal requirement, to inform the person that their information has been disclosed. If it is not appropriate to inform the person the Privacy and Complaints Officer should be consulted. The fact that the information has been disclosed, the reasons why it was disclosed, and why the person was not informed of the disclosure should be recorded in the person’s Manaaki or HR file.
- 13.16 A summary of the more common statutory provisions that require information requested to be provided are set out below:
- (a) **Health Act 1956 - Section 22F:** If NZALS receives a request for health information from the person concerned, the person’s representative, a caregiver, or any other organisation or person who is, or who will be providing, health services to the person, the provisions in section 22F of the Health Act will apply. NZALS must provide the information unless one of the exceptions in section 22F(2) apply. For more information on responding to a request under section 22F refer to ‘Requests under section 22F of the Health Act’ later in this Policy.
  - (b) **Health Act 1956 - Section 22D:** The Minister of Health can require disclosure of health information under section 22D of the Health Act 1956 provided the criteria in that section are met. The information provided must not identify an individual unless the person (or his or her representative) consents to the disclosure, or the identifying information is essential for the purposes for which the information is sought.

- (c) **Health and Disability Commissioner Act 1994:** The Health and Disability Commissioner may, by notice in writing, require any person to give information and provide documents relating to any matter under investigation by the Commissioner with limited exceptions.
- (d) **Coroners Act 2006:** The Coroner may require information and documents to be provided for the purposes of an inquest.
- (e) **Privacy Act 1993:** The Privacy Commissioner may require information for the purpose of conducting investigations under the Privacy Act or HIPC.

### Is there discretion to disclose?

13.17 NZALS **must not** disclose the information unless an exception in Rule 11 of the HIPC, Principle 11 of the Privacy Act, or another statute allows the disclosure.

13.18 The exceptions in Rule 11 that are most likely to apply if NZALS wants to disclose health information include:

- (a) **the disclosure is to, or is authorised by,** the person concerned, or their representative where the person is dead or is unable to exercise his or her rights under the HIPC (Rule 11(1)(a) and Rule 11(1)(b) respectively);
- (b) **the disclosure is one of the purposes** in connection with which the information was obtained. The person must have been informed of the purpose when the information was collected (Rule 11(1)(c));
- (c) **NZALS obtained the information from a publicly available publication** (Rule 11(1)(d));
- (d) where NZALS believes on reasonable grounds that it is either **not desirable or not practicable to obtain authorisation from the person concerned** (for example the person might be unconscious or not competent), Rule 11(2) of the HIPC allows disclosure where:
  - i. **the disclosure is for a directly related purpose** in connection with which the information was obtained (Rule 11(2)(a));
  - ii. **the information is disclosed by a ‘health practitioner’ to a person closely associated with the patient.** The person receiving the disclosure must be a contact person (i.e. named as contact on a consent form or service agreement), principal caregiver or a near relative. The disclosure must be in line with recognised practice, and not be contrary to the express veto by the person concerned or their representative (where the patient is not competent to make a decision). This exception only applies to health practitioners registered under the HPCA Act (Rule 11(2)(b));

iii. **the disclosure is necessary to prevent or lessen a serious threat** (Rule 11(2)(d)).

To rely on this exception:

- the threat must be serious; and
- the threat must be to public health or safety, or the life or health of the person or another person; and
- the information must be given to someone who can act to prevent or lessen the threat (such as the Police or a CYFS social worker); and
- only the information necessary to achieve that purpose may be given (Rule 11(3))

Note: Serious is defined in section 2 of the Privacy Act and means a threat NZALS reasonably believes to be serious having regard to:

- the likelihood of the threat occurring; and
- the severity of the consequences if it did occur; and
- the time at which the threat may occur (when is it likely to happen);

iv. **the disclosure is necessary to avoid prejudice to the maintenance of the law** by a public sector agency or for the conduct of court or tribunal proceedings (Rule 11(2)(i));

v. **the information will be used in a form that does not identify the person concerned or for research and statistical purposes**, and will not be published in a form which could identify the person, and ethical committee approval has been obtained if necessary (Rule 11(2)(c)).

13.19 **Employee information** about an identifiable employee is personal information and will be governed by the Principles in the Privacy Act. Principle 11 has similar, but slightly different exceptions to those set out above for Rule 11. Where NZALS wants to, or is asked to, disclose information about an employee (as defined in this Policy) an exception in Principle 11 of the Privacy Act, or some other statutory provision allowing the disclosure must apply.

13.20 If an exception in Rule 11, Principle 11, or a statute applies, the exception allows NZALS to make the disclosure; it does not require NZALS to do so. For instance NZALS may decide not to disclose the information because the ethical code of the particular health professional or duties of confidentiality impose stricter limits on disclosure.

13.21 The decision whether or not to disclose, when permitted by Rule 11 or Principle 11 (or any other statute that allows but does not require disclosure) remains with NZALS.

### Is the information disclosed appropriately, proportionately and securely?

13.22 When disclosing information under Rule 11, Principle 11 or any other statutory provision, care must be taken to provide only the information that NZALS is permitted to provide under the relevant provision:

- (a) under Rule 11(3) only information necessary for the purpose for which it is being disclosed should be disclosed;
- (b) where health information is requested under sections 22C or 22F of the Health Act it is important to remember that the definition of health information in the Health Act is narrower than in the HIPC (refer to definitions section of this Policy).

13.23 Any decision to disclose information must be made in accordance with: the Rules in the HIP Code, Principles in the Privacy Act, or the relevant provision in a statutory authority you are relying on; and this Policy. This will include considering if the intended disclosure is **reasonable in all the circumstances** including ensuring:

- (a) where you are relying on the consent of the person to disclose the information, any limits or restrictions imposed by the person as to what information can be disclosed is understood and adhered to;
- (b) only information necessary for the purpose is disclosed;
- (c) distinguishing clearly between fact and opinion where that is relevant;
- (d) disclosing the information only to the person(s) who need to know and who can do something to mitigate or eliminate any risk;
- (e) checking that the information is accurate and up-to-date before disclosure;
- (f) only disclosing information in a secure manner and ensuring the recipient of the information understands any limits to any consent to the disclosure.

13.24 Where information is released to someone else NZALS must take all reasonable steps to ensure the information is transferred in a way that preserves privacy (e.g. clinical records should not be sent by ordinary mail, information sent on a memory stick should be encrypted).

### Has the decision been properly recorded?

13.25 It is important that a decision to disclose or not to disclose is recorded including:

- (a) the request (who made the request, the date of the request and the actual information sought);
- (b) the provision in the HIPC, Privacy Act or other statutory authority relied on;
- (c) what information was disclosed (if any), what information requested was not disclosed (if any) including the reason why the information was not provided, and the date the information was provided;
- (d) who made the decision on whether the information would be disclosed or not;
- (e) how the information was provided to the person.

## Process to follow where NZALS receives a request for disclosure

13.26 All requests made to NZALS for disclosure of information:

- (a) must be put in writing (email is fine) to avoid a dispute at a later date;
- (b) must be referred to the Privacy and Complaints Officer to be logged in NZALS' system. The Privacy and Complaints Officer will then work with the appropriate manager and/or health professional to determine what if any information is to be released;
- (c) must be recorded in the patient's Manaaki file (refer para 14.25 above)

13.27 If the decision is made to disclose the information it is important to:

- (a) identify the precise provision in the Privacy Act, HIPC or other statute you are relying on to disclose the information;
- (b) identify precisely what information should be disclosed;
- (c) identify who the information is being disclosed to;
- (d) ensure that any information disclosed is disclosed securely;
- (e) ensure the decision-making process and the reasons for disclosure have been recorded in the patient's Manaaki file (refer para 14.25);
- (f) seek advice if necessary.

## Specific disclosure situations

### Requests for disclosure by the person concerned or their agent

13.28 If a request is made by the person concerned or their properly authorised agent the request comes under section 22F of the Health Act and must be dealt with as a request under section 22F of the Health Act (Refer to 'Requests under section 22F of the Health Act' below).

13.29 A person, who is competent, can consent to, or authorise any third party, such as a relative, interpreter, insurer, to have access to their information. Where a person has asked for a third party to be given access to their health information it is advisable to seek this request and authorisation in writing. The exact nature of the information the person wants disclosed to the third party should be clearly recorded, and the information should be checked to ensure only relevant information that falls within the request is disclosed.

13.30 If the person nominates another person to act as their agent, the agent can authorise the disclosure of any information relating to the person for whom they are acting, within the delegation given to them by the person concerned.

13.31 If an agent is acting for the person, NZALS will require written authorisation from the person concerned that:

- (a) the person nominated as the person's agent has the authority to act as their agent; and
- (b) in what circumstances and for what information the person is authorised to act on the person's behalf.

13.32 Care must also be taken not to inadvertently disclose information about other persons, (i.e. 'mixed information') that could be on the person's record.

#### Disclosure to a 'representative' including parents or guardians of a child under 16 years

13.33 A person has the following people as his or her representative(s):

- (a) if the person is deceased, the administrator or executor of the estate;
- (b) if the person is under 16 years of age, his or her parents or guardians;
- (c) if the person is not a person described in (a) or (b) above and is unable to give consent or exercise rights, a person appearing to be lawfully acting on his or her behalf or in his or her interests (e.g. a welfare guardian or enduring power of attorney).

13.34 Information can be disclosed to a person's 'representative' or disclosure can be authorised by the representative **if the person concerned is unable to exercise their rights under the HIPC** (Rule 11(1)(a) and(1)(b) of the HIP Code).

13.35 Under section 22F of the Health Act a representative can directly request access to information about the person. Refer to 'Requests under section 22F of the Health Act' below.

13.36 Section 22F of the Health Act only applies where **a request has been received** for information about the person concerned from a person authorised under the section. If NZALS wishes to disclose information to a representative, including a parent or guardian, without a request, or where the child is 16 years or over, then the disclosure must come within one of the exceptions in Rule 11 of the HIPC.

13.37 Difficult situations can arise when a child or young person has the capacity to understand their rights under the HIPC, and refuses to have their health information shared with their parent or guardian. While in most cases information will, and should be shared with a child's parents, parents do not have an automatic blanket right to all health information about their children. Where there is any conflict or concern the Privacy and Complaints Officer should be consulted.

### Disclosure to other family, caregivers and friends

- 13.38 If NZALS receives a request for health information from a family member or other person close to a patient the first step is to seek authorisation from the patient. If the patient is happy for the information to be released it can be (Rule 11(1))(b).
- 13.39 Health information can only be disclosed to family, partners or close friends, without the person's consent, if one of the exceptions in Rule 11 applies. The following exceptions may apply to NZALS:
- (a) where that use or disclosure was one of the purposes for which the information was obtained and the person is made aware of this purpose at the time the information was collected (Rule 11(1)(c));
  - (b) where it isn't desirable or practicable for a health practitioner to get the person's permission for disclosure, information about the person can be disclosed to the person's:
    - i. principal caregiver;
    - ii. near relative;
    - iii. nominated contact person.

Note: Disclosure under this exception can only be made by a health practitioner registered under the HPCA Act, must be in line with recognised professional practice, and information must not be disclosed if the person vetoes the disclosure (Rule 11(2)(b)).

### Disclosure to caregivers providing services to the person

- 13.40 If a caregiver providing care to a person (including a family member who is providing care to the person) requests that person's health information the request must be dealt with under section 22F of the Health Act. (Refer to 'Requests under section 22F of the Health Act' below).
- 13.41 NZALS can disclose relevant information to a person's caregivers without a request where this was one of the purposes for which the information was obtained, and the person was informed that this would occur (Rule 11(1)(c)).
- 13.42 If neither of the above applies information **must not be disclosed** unless another exception in Rule 11 applies, or the person concerned consents to the disclosure.

### Requests from other health or disability service providers

- 13.43 Other health and disability service providers may use section 22F of the Health Act to **request** appropriate information from NZALS. If a request for information is received from another health provider it must be considered under section 22F (refer below).

### Requests under section 22F of the Health Act 1956

- 13.44 The Privacy and Complaints Officer should always be consulted prior to making a decision under section 22F of the Health Act.
- 13.45 Section 22F only applies to **requests** for information and cannot be used to voluntarily disclose information where a request for the information has not been made.
- 13.46 There are three parties who may make a request for health information under section 22F of the Health Act:
- (a) **the person concerned or their agent** - Rule 11(4)(a) of the HIPC requires the request to be treated as an access request under Rule 6 of the HIPC;
  - (b) **representatives**, as defined under the HIPC and Health Act (refer to definitions section in this Policy);
  - (c) **any other person or agency that is providing, or is to provide health services to the person.**
- 13.47 If NZALS receives a request under section 22F the information **must** be provided unless a withholding ground applies. If a withholding ground applies, NZALS **may** withhold the information if it wishes, but does not have to do so.
- 13.48 If the request causes any concern further advice may be required. Concerns may arise where: the request is very broad or includes information that does not appear to be relevant or necessary for the requestor in order to provide services to the patient, or that would more appropriately be released by another provider (i.e. records held by NZALS and obtained from a DHB).
- 13.49 If NZALS discloses information in excess of what can lawfully be disclosed under section 22F or refuses to disclose the information requested it could be subject to a complaint to the Privacy Commissioner.
- 13.50 When NZALS receives a **valid request** from any of the three parties that may make a request under section 22F it **must** disclose the relevant information **unless**:
- (a) NZALS has a lawful excuse not to disclose (e.g. a statutory obligation of confidentiality, legal privilege, or a ground in sections 27 – 29 of the Privacy Act); or
  - (b) Refusal of the request is authorised by a Rule in the HIPC.
- 13.51 If the request is from the person's representative the request may be refused on the above grounds or where:
- (a) it would be contrary to the 'interest' of the person concerned to disclose the information (e.g. abuse by the representative is suspected); or
  - (b) NZALS has reasonable grounds for believing that the person concerned does not, or would not; wish the information to be disclosed.

- 13.52 If the request is by a person or organisation who is providing, or is to provide, health services to the person NZALS **may** refuse to disclose the information on one of the grounds set out in para 14.50 or where NZALS has reasonable grounds for believing that the person does not or would not wish the information to be released (e.g. if NZALS has reason to believe the patient would veto the disclosure if asked).
- 13.53 **If any of the circumstances above apply** NZALS has discretion whether or not to withhold the information. NZALS may still provide the information if it believes in the circumstances that is the appropriate action.
- 13.54 If **none of the grounds** for refusing the request above apply NZALS **must** disclose relevant information in accordance with the request.
- 13.55 Under section 22F and Rule 11(4) of the HIPC all representatives have the same right to request access to the health information of the person concerned. A request by one representative cannot be vetoed by another (refer to Case note 231747 [2011] NZ PrivCmr 8, on the Privacy Commissioner's website).
- 13.56 In most circumstances it will be good practice, and may be required under some health professionals' Codes of Ethics, to speak with the patient about the request before responding to the request where this is practicable and appropriate. While there is no legal requirement to obtain the patient's authorisation to the disclosure of the information and the patient cannot veto the disclosure, if the patient did not want the information disclosed this is an important factor that NZALS should take into account in determining whether to refuse a request by a representative or other health provider.
- 13.57 There is no requirement in section 22F that the request must be in writing, or refer to section 22F. However, NZALS' policy is that if the request is not made in writing the requestor must be asked to put the request in writing (by email is fine) to avoid any dispute at a later date. A record of the request must be kept on the patient's Manaaki file, including what information was disclosed under the request.

#### Requests under section 22C of the Health Act 1956

- 13.58 The Privacy and Complaints Officer should always be consulted prior to making a decision under section 22C of the Health Act.
- 13.59 When NZALS receives a request for health information about a person from someone listed in section 22C(2) of the Health Act, it has a **discretion** whether or not to provide the information. The information must be required for the person to carry out their powers, duties and/or functions as set out in section 22C(2).
- 13.60 Section 22C of the Health Act **allows** information to be disclosed in response to a request. It does not require NZALS to provide the information, or allow information to be volunteered without a request.

13.61 Some of the categories of people listed in section 22C are:

- (a) police officers;
- (b) medical officers of penal institutions;
- (c) probation officers;
- (d) CYFS social workers and care and protection co-ordinators.

13.62 Information may also be disclosed to the employees of a DHB (section 22C(2)(j)). But in these cases disclosure of identifiable information must be essential for carrying out the DHB's powers, duties or functions under the New Zealand Public Health and Disability Act 2000.

13.63 If the request is not made in writing NZALS will ask the requestor to put the request in writing (by email is fine) to avoid any dispute at a later date.

13.64 In all cases it is important that only the information authorised to be disclosed under this section is disclosed, and that a record of the information request, and information disclosed is kept on the patient's Manaaki file.

13.65 Consideration should be given to informing the patient of the request unless doing so may prejudice the purpose for which the information was requested. A patient cannot veto the release of the information requested. However, if it is appropriate to inform the patient of the request, the patient's views are an important factor NZALS should take into account when exercising its discretion to release the information.

#### Requests under the Official Information Act 1982 ('OIA'), including requests from a third party (not a representative or agent of the person concerned)

13.66 NZALS is subject to the OIA. All information held by NZALS (including health information) is official information under the OIA. Requests for information about NZALS itself must be dealt with as an OIA request.

13.67 If a **third party** requests information about another person, and is not acting as the other person's agent, or representative, the request **must** be dealt with under the OIA. The request must be referred to the Privacy and Complaints Officer.

13.68 Refer to the **Official Information Policy** for guidance on managing an OIA request.

#### Disclosure of a deceased patient's health information

13.69 Health professionals' ethical and professional obligation of confidentiality does not cease after the professional relationship ends or a patient dies. In addition, information held by NZALS continues to be covered by Rule 11 of the HIPC for 20 years beyond the death of a person (or until it is no longer kept by NZALS) (Rule 11(5) and (6)).

13.70 Any request for a deceased patient's health information must be referred to the Privacy and Complaints Officer.

- 13.71 All the exceptions in Rule 11 will apply and it may not always be necessary to obtain authorisation from the deceased's representative.
- 13.72 If a request is received by the deceased person's representative this must be managed as a request under section 22F of the Health Act. The representative will normally be the person's executor(s) or administrator(s) of their estate, or the parent or guardian of a deceased child under 16 years. Refer to section 'Requests under section 22F of the Health Act' in this Policy for further information on how to respond to a request by a representative.
- 13.73 The representative must be asked to provide evidence that they are either an executor or administrator of the deceased's estate, or the parent or guardian of the child if the deceased is a child under 16 years. If the person is an Executor of the deceased's will a copy of the Grant of Probate should be sighted, if the representative is an Administrator of the estate a copy of the Grant of Letters of Administration must be sighted. In either case a copy of the required documentation must be kept with the deceased's health information.
- 13.74 If a request is received for a deceased patient's information by anyone other than the person's representative, the request must be decided under the OIA. Refer to the section 'Requests under the Official Information Act 1982' above and the **Official Information Policy**.
- 13.75 For information on how a deceased patient's records are managed by NZALS refer to the **Management of Deceased & Inactive Patient Records** procedure.

#### Where a person vetoes disclosure

- 13.76 If information was obtained for a particular purpose, including disclosure to a caregiver, and the person was aware of this purpose at the time the information was collected, disclosure of that information may usually be made under the HIPC or Privacy Act despite the person later vetoing the use or disclosure.
- 13.77 Where the purposes do not include disclosure of certain information, NZALS must consider whether one of the exceptions in the HIPC or Privacy Act applies and would allow the proposed disclosure when the patient has vetoed it.
- 13.78 Special care should always be taken in this situation. A health professional's ethical obligations may preclude use or disclosure of the information in these circumstances, and/or even where it is permissible to use or disclose the information, this may not be the appropriate course of action.
- 13.79 The Privacy and Complaints Officer should always be consulted in this situation.

## 14 Managing a data or privacy breach or complaint

### Managing a privacy breach

- 14.1 A 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.
- 14.2 The Office of the Privacy Commissioner has developed guidance material for organisations managing a privacy breach. This includes 'Privacy Breach Guidance Material Key Steps for Agencies in Responding to Privacy Breaches' and a 'Privacy Breach Checklist.' These guidelines are available on the Privacy Commissioner's website and **will be used by NZALS in managing any privacy breach situation.**
- 14.3 The guidelines set out four key steps to consider when responding to a privacy breach or suspected breach:
- (a) **Containment** – Take appropriate action to contain the breach and undertake a preliminary assessment;
  - (b) **Evaluation** of the risks associated with the breach;
  - (c) **Notification** - Determine who needs to be notified and how that notification should occur; and
  - (d) **Prevention** – Take appropriate action to prevent a repeat of the breach.
- 14.4 Steps 1, 2 and 3 should be undertaken either simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and prevention strategies. The decision on how to respond should be made on a case-by-case basis.
- 14.5 The Privacy and Complaints Officer is responsible for managing the response to all privacy breaches.
- 14.6 At the date this Policy came into force there is no mandatory requirement to notify the Office of the Privacy Commissioner, or persons affected of a data breach. However, it is often good practice to notify the Commissioner and potentially affected person(s) when investigating and managing a suspected privacy breach (e.g. voluntary breach notification). The CEO will make the decision whether or not to inform the Privacy Commissioner and/or potentially affected person(s).

Note: Proposed changes to privacy legislation are likely to include a mandatory reporting of data breaches to the Office of the Privacy Commissioner and in serious cases the person(s) concerned. The Privacy and Complaints Officer must check if mandatory reporting has been introduced when managing any data breach under this Policy.

## Managing privacy concerns and complaints

- 14.7 The Privacy and Complaints Officer is responsible for managing privacy concerns and complaints. He/she will decide whether or not a case can be handled individually or escalated for an inquiry process. A complaint of a breach of the HIPC must be managed in accordance with the requirements in clause 7 of the Code (page 75 of the HIPC) and as set out in the NZALS **Complaints Policy**.

## 15 Specific responsibilities

Party	Responsibilities
All Employees	<ul style="list-style-type: none"> <li>• Understand their obligations and person's rights under privacy legislation and their professional standards</li> <li>• Follow NZALS Privacy Policy and relevant procedures</li> <li>• Ensure all information requests are forwarded to the Privacy and Complaints Officer</li> <li>• Inform the Privacy and Complaints Officer and manager of any privacy breach or complaint</li> </ul>
Privacy and Complaints Officer	<ul style="list-style-type: none"> <li>• Is familiar with the privacy principles in the Privacy Act and HIPC, and other legislation governing what NZALS can and cannot do with personal information</li> <li>• Manages concerns or complaints from patients about issues to do with privacy</li> <li>• Deals with requests for access to personal information, or correction of personal information and ensuring timeframes in the HIPC and Privacy Act are met</li> <li>• Advises managers on how to ensure NZALS' business practices comply with privacy requirements</li> </ul>
Chief Executive and Regional Managers	<ul style="list-style-type: none"> <li>• Ensure all personnel are aware of, have training in, and comply with this Policy, and their obligations under privacy law and relevant professional standards</li> <li>• Ensure all privacy protection guidelines are adhered to by centres</li> </ul>
The Board	<ul style="list-style-type: none"> <li>• Provide responsible governance and monitoring of compliance with legal and professional obligations</li> </ul>

## 16 Legal compliance

- [Health Information Privacy Code 1994](#)
- [Privacy Act 1993](#)
- [Public Records Act 2005](#)
- [Health Act 1956](#)
- [Health \(Retention of Health Information\) Regulations 1996](#)
- [Official Information Act 1982](#)
- [Health and Disability Commissioner Act 1994](#)
- [Coroners Act 2006](#)
- [Code of Health and Disability Services Consumers' Rights](#)
- [SSC Code of Conduct](#)
- *ACC Contract – on file*
- *MoH Contract – on file*

## 17 Related Policies, Procedures and Forms

- [Data Protection Policy](#)
- [Mobile Device Usage Policy](#)
- [Code of Conduct Policy](#)
- [Discipline Policy](#)
- [Internet and Email Use Policy](#)
- [Official Information Act Policy](#)
- [OIPC - Privacy Breach Checklist](#)
- [Privacy Statement and Privacy Consent Form](#)
- [NZALS Privacy Request procedure](#)
- [Responding to privacy information requests: letter templates 1-4](#)
- [Management of Deceased & Inactive Patient Records](#)
- *Records Management Policy*
- *Retention & Disposal Procedures*

## 18 Revision History

Author	Version number	Version date	Description of changes
Compliance Advisor	3.1	August 2016	Breach links updated
Claro Law	3.0	November 2015	Updated policy
Communications & Reporting	2.1	February 2014	Updated policy