PRIVACY POLICY AND GUIDELINES

PURPOSE AND SCOPE OF POLICY

All references to Access Community Health in this document refer to Access and Total Care Health services.

The purpose of this document is to outline Access Community Health's policy in respect of our obligations under the Privacy Act 2020 and Health Information Privacy Code 2020.

This document:

- sets out Access Community Health's policy framework for managing personal information and protecting individuals' privacy;
- applies to all Access Community Health employees, contractors, and subsidiaries;
- applies to all personal information held by Access Community Health, including information pertaining to both employees and service users;
- specifies who Access Community Health's Privacy Officer is and their role in that regard;
- confirms Access Community Health's approach to privacy issues arising (including requests to access information, disclosures and complaints); and
- provides an appropriate framework to ensure possible privacy breaches are investigated appropriately in a fair, equitable, timely and consistent manner.

<u>Guidelines</u>

This document has been developed to provide general guidelines on privacy matters and has been developed and adapted from the Office of the Privacy Commissioner's resources, including *"On the Record – A Practical Guide to Health Information Privacy"*.

All references to 'personal information' include 'health information' in this document. All references to 'information' generally in this document refer to both personal and health information for the purposes of the Privacy Act 2020 and the Health Information Privacy Code 2020.

CONTENTS

PRIVACY OFFICER

Access Community Health's Privacy Officer is the National Health and Safety Manager, based in Auckland.

The Privacy Officer's contact details are:

Email: privacy@access.org.nz

The Privacy Officer's duties include:

- responsibility for this Policy;
- maintaining a Privacy Register outlining privacy matters for the organisation (including a record of complaints, education and advice provided);
- maintaining oversight of, and acting as liaison with, subsidiaries and their related privacy officers in relation to ongoing privacy management;
- managing the process for handling requests to Head Office for access to personal information;
- managing complaints in respect of Access Community Health regarding personal information and the Privacy Act or Health Information Privacy Code;
- managing privacy disclosures/breaches and related privacy inquiries in relation to Access Community Health;
- managing Access Community Health's relationship with the Office of the Privacy Commissioner (including all communications with this office); and
- oversight of training and education of employees and subsidiaries in relation to this Policy and privacy-related matters; and
- ensuring Access Community Health's compliance with the Privacy Act and Health Information Privacy Code.

The Privacy Officer function may be delegated from time to time.

The Privacy Officer will also maintain a close link with Green Cross Health's Privacy Officer who has responsibility for other parts of the Green Cross Health group.

Access Community Health Employees responsibility

All – privacy training is to be undertaken as part of induction and for Support Workers, this is included in their Support Worker training.

Non-support worker - Every employee of Access Community Health is required to undertake Privacy Act training via Teach Me within a month of starting their employment.

COMPLIANCE WITH THE ACT AND CODE

The organisation will comply with the Act and Code, and in particular the Information Privacy Principles. These principles are summarised below, and then explored further in the following sections.

Principle 1

Personal information must only be collected when:

- The collection is for a lawful purpose, connected with what Access Community Health does, and
- It is necessary to collect the information for that purpose.

Principle 2

Personal information must usually be collected from the person the information is about. But sometimes it is all right to collect information from other people instead - for instance, when:

- Getting it from the person concerned would undermine the purpose of the collection
- It's necessary so a public sector body can uphold or enforce the law
- The person concerned authorises collection from someone else.

Principle 3

When Access Community Health collects personal information from the person the information is about, it has to take reasonable steps to make sure that person knows things like:

- Why it is being collected
- Who will get the information
- Whether the person has to give the information or whether this is voluntary
- What will happen if the information isn't provided.

Sometimes there are good reasons for not letting a person know about the collection, for example, if it would undermine the purpose of the collection, or it's just not possible to tell the person.

Principle 4

Personal information must not be collected by unlawful means or by means that are unfair or unreasonably intrusive in the circumstances.

Principle 5

It's impossible to stop all mistakes. But Access Community Health must ensure that there are

reasonable safeguards in place to prevent loss, misuse or disclosure of personal information.

Principle 6

Tangata/people have a right to ask for access to personal information that identifies them.

Access Community Health may refuse to give access to information in some circumstances, for instance because giving the information would:

- endanger a person's safety
- prevent detection and investigation of criminal offences
- involve an unwarranted breach of someone else's privacy.

Principle 7

Tangata/people have a right to ask Access Community Health to correct information about themselves, if they think it is wrong.

If Access Community Health does not want to correct the information, it does not usually have to. But tangata/people can ask us to add their views about what the correct information is (and hold it on file).

Principle 8

Before Access Community Health uses or discloses personal information, we must take reasonable steps to check that information is accurate, complete, relevant, up to date and not misleading.

Principle 9

Access Community Health must not keep personal information for longer than is necessary for the purposes for which the information may be lawfully used.

Principle 10

Access Community Health must use personal information for the same purpose for which we collected that information.

Other uses are occasionally permitted (for example because this is necessary to enforce the law, or the use is directly related to the purpose for which we got the information originally).

Principle 11

Access Community Health can only disclose personal information to other parties in limited circumstances. One example is where another law requires us to disclose the information. Also,

Access Community Health may disclose information if we reasonably believe, for example, that:

- disclosure is one of the purposes for which we got the information in the first place;
- disclosure is necessary to uphold or enforce the law;
- disclosure is necessary for court proceedings;
- the person concerned authorised the disclosure;
- the information is going to be used in a form that does not identify the person concerned.

Principle 12

An agency may only send personal information to another country if that country has similar levels of privacy protection to New Zealand, or the person concerned is fully informed and gives their permission.

Principle 13

Some agencies give people a "unique identifier" instead of using their name. Examples are NHI numbers in the health sector, a driver's licence number, a student ID number, or an IRD number. People should not be required to disclose their unique identifier unless this is one of the purposes for which the unique identifier was set up (or directly related to those purposes).

1. COLLECTION OF PERSONAL INFORMATION

Access Community Health will only collect personal information that is connected with Access Community Health's business.

When information is collected, the purposes for collection and proposed use of that information will be explained to the person whose information it relates to.

Consent

It is important that individuals are aware that we are collecting their personal information and they must provide their consent in that regard. They are also entitled to withhold consent to such collection. In these circumstances, further advice should be sought from the Privacy Officer.

Consent for a third party to access personal information

At the point of collection of personal information, sometimes an individual will provide consent for someone else to access their personal information (e.g. next of kin). That consent must be recorded in writing.

Employment Induction

All new employees will be informed that their personal information is being collected for employment purposes, and who will access and use that information.

Service User Agreements

All service user agreements (or similar documentation) will contain a clause stating that personal information may be shared with other health providers for the purpose of delivering appropriate support and ensuring the health and safety of the service user. This clause should not be varied by a service user without the Privacy Officer's review and approval.

2. SOURCE OF PERSONAL INFORMATION COLLECTED

Where possible, Access Community Health will collect personal information about employees and service users directly from those individuals.

In some limited circumstances, Access Community Health may collect information about a person from someone other than the person it relates to. Some examples include:

- when a service user has authorised collection from someone else (e.g. a whānau/family member, advocate or friend).
- referral information from a funder (including from a NASC).

- in some circumstances, collecting information directly from service users may prejudice their interests or the purpose of collection (such as treatment), or it may prejudice the safety of another person – in this type of case, Access Community Health may collect the required information from a third party. If the service user cannot be found or contacted, or does not know the information sought, Access Community Health may seek the information elsewhere.
- when another person's perspective on a person's health conditions and the effect of particular medication or treatment may be required.
- if it is believed on reasonable grounds that a service user might not be telling the truth or (in rare circumstances) may have refused to provide the information and this information is considered necessary.

Where information is collected from someone other than the person the information relates to, Access Community Health will check the accuracy of the information collected with the individual concerned where possible (and appropriate) and record this in writing.

2.1. Other Health Providers

Access Community Health may need to collect personal information about a service user from other health agencies. Other health agencies may also seek to collect personal information from Access Community Health regarding our service users.

Section 22F of the Health Act 1956 requires health information to be provided to a health agency that is providing, or is to provide, services to that individual, on request from the agency, except in some limited circumstances (see below). If it is not passed on when it should be, a complaint can be made to the Privacy Commissioner.

Right 4(5) of the Code of Health and Disability Services Consumers' Rights gives service users the right to cooperation among providers to ensure quality and continuity of services. Co-operation would include sharing appropriate information with other providers, and this sort of information sharing will often be one of the purposes for which information is collected. If information is not passed on when it should be, consumers can complain to the Health and Disability Commissioner.

In these types of cases, it can be a difficult decision when trying to choose whether or not to disclose certain information – employees and subsidiaries are encouraged to consult with the Privacy Officer in these circumstances.

2.2. Family Members and Employers Providing Information

Access Community Health may receive information about service users from family members or employers, on the basis that the information (and who provided it) will be kept secret. However, a promise of confidentiality to someone (such as a family member) who has provided information about a service user will not necessarily be recognised as a withholding ground if the service user later requests access to the information. Because of this, such promises of secrecy regarding information collection should not be made.

3. COLLECTING PERSONAL INFORMATION FROM THE INDIVIDUAL CONCERNED

Where Access Community Health collects personal information directly from individuals, we will ensure the individual is aware of:

- the fact information is being collected;
- the purpose of collection (e.g. for care and treatment and related administrative purposes);
- the intended recipients of the information (e.g. Access Community Health employees, the relevant funding provider such as a DHB, Ministry of Health or ACC, the person's GP, and the person's family members and other carers if that is acceptable to the service user);
- the consequences of not supplying the information (i.e. there may be problems if the service user does not provide full or accurate information. For instance, a particular treatment may not able to continue effectively without complete and accurate information. Or if the service user has applied for a subsidy or benefit, it may not be possible to process the claim without complete and accurate information); and
- the service user's rights of access and to seek correction.

3.1. Exceptions to Collection from the Individual Directly

In some limited circumstances, Access Community Health may not need to explain to a service user the details around information collection (outlined above). For example, where:

- compliance with this rule by Access Community Health would prejudice the interests of the service user or prejudice the purposes of collection (e.g. if a fully informed service user would be likely to behave in a way that prevents their condition being effectively assessed, or in a way that is against their own interests); or
- compliance is not reasonably practicable in the particular circumstances. For instance, where:
    - an explanation would unreasonably delay the provision of necessary emergency treatment;
    - the service user is not able to take in an explanation when it is offered because of their mental or physical state; or
    - the explanation might cause a violent reaction.

If Access Community Health cannot give the necessary explanation when the information is collected, this should be done as soon as possible afterwards (where appropriate). However, repeat explanations are not necessary, assuming the purpose for collection is unchanged.

3.2. Photographs and recordings

Any photograph or recording taken of a service user or employee is personal (and likely health) information and is subject to the same privacy and confidentiality principles as other personal and health information.

When collecting and/or sharing photographs or recordings, as with all other personal and health information, there are legal, professional, and ethical responsibilities to be met.

The collection, use, storage, retention, and disclosure of photographs and recordings about an identifiable individual is governed by the Act and the Code, in the same way as all other personal and health information.

In respect of employees, the relevant manager must ensure that the employee is aware that their photo is being taken, or that they are being recorded, and what the intended use is going to be. They must be aware and have a chance to say whether or not they are comfortable with that. If an employee indicates that they do not wish to be photographed or recorded as proposed, their choice must be respected.

In respect of service users, consent from the individual (or their legal representative) must be obtained on the Consent to Photographs and Recordings form.

A photograph or recording must only be taken for appropriate purposes which the service user has been informed of, and agrees to, and:

- must only be used for the purpose for which it was obtained or a directly related purpose;
- can only be used for another purpose if the service user consents to the use, or the use is permitted by the Act, the Code, or any other statutory provision;
- must be stored securely against unauthorised access or use (e.g. if kept on a USB stick encrypted, stored securely i.e. in a locked cabinet).

Access Community Health does not permit service user photography or recordings to be taken on personal devices, including smart phones. Only approved organisation devices (and apps) must be used. Where exceptional circumstances arise in which it may be necessary to take a photo or recording on a personal device, this should be discussed with the relevant manager first.

If a photograph or recording is to be used for anything other than clinical care and maintaining a record in the clinical record the service user must have given explicit consent for the additional use. This includes uses such as training and education, publication, promotion, and research. The service user's consent must be recorded in their clinical record.

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.

Uploading recordings or photos to any social media platform of service users / clients, whānau and their homes is prohibited.

4. MANNER OF COLLECTION OF PERSONAL INFORMATION

Access Community Health will ensure that personal information will be collected using methods that are lawful, fair and do not intrude to an unreasonable extent on the affairs of the individual concerned.

When collecting health information (or any information of a sensitive nature), Access Community Health will ensure that an individual has physical privacy to provide that information, where possible. (For service users, physical privacy is protected by right 1(2) of the Code for Health and Disability Services Consumers Rights.) For example, employees and/or service users should not be asked to provide or clarify personal information when standing in a reception or other public area where other people may hear the discussion.

5. STORAGE AND SECURITY OF PERSONAL INFORMATION

Access Community Health will take reasonable security safeguards with personal information against its:

- loss
- access, use, modification, or disclosure without Access Community Health's authority; and/or
- other misuse.

Where Access Community Health gives personal information (or access to personal information) to a third party (for example, an IT contractor), it will ensure a non-disclosure or confidentiality agreement is signed to prevent unauthorised use or disclosure of information by that person or organisation.

Access Community Health's approach to security of information is as follows:

1. All locations containing information in hard copy will be secure with lock, keypad or swipe card access.
2. All filing cabinets and unattended rooms (containing information) will be secure/locked at all times and associated keys stored appropriately.
3. Computer screens will be positioned so they cannot be seen or accessed by unauthorised personnel.
4. Screen savers and security screens will be used so computer terminals cannot be seen by visitors or unauthorized personnel and will be required when employees leave their desk unattended for any period of time.
5. A "clear desk" approach will be taken by all employees working in an 'open' office space so that no work-related documents are left unattended and open to perusal by other people who may not be authorised.
6. Personal information disclosed to funders or other health agencies will be transferred via a secure communication and marked as "strictly confidential" and all documents must be password protected.

7. Any personal information transported by employees outside of the office in hard copy or via laptop or other device (e.g. phone or tablet) will be secure at all times (e.g. in a secure bag or folder kept out of sight in a locked vehicle). It is the preference of Access Community Health that hard copy documentation should only be transported outside of the office if absolutely necessary.
8. No service user personal information is to be stored at any time on employees' personal/home computers or devices (e.g. phone or tablet).

Refer separate ICT policy regarding further details on Access Community Health's general security safeguards.

6. RETENTION OF PERSONAL INFORMATION

Access Community Health will not retain personal information for longer than is required for the purposes for which it may lawfully be used.

When all purposes for holding the personal information have expired, including the obligatory retention period under the Health (Retention of Health Information) Regulations set out below, the information will be securely destroyed (or returned to the service user if requested to do so).

If the relevant time period is not stated on a particular document, the default retention period will be 10 years.

Health (Retention of Health Information) Regulations 1996

The Health (Retention of Health Information) Regulations require all health information held by a services provider to be kept for at least ten years from the last date services were provided to the individual. These Regulations apply to health information held by Access Community Health.

These Regulations allow information to be transferred to another provider in this time period, so if a service user moves to another town the records can be forwarded to a new doctor or health provider.

The Regulations also allow agencies to transfer information to the service user or (where the service user has died) to the executor of their estate.

7. ACCURACY OF PERSONAL INFORMATION

Before using personal information collected from service users or employees, Access Community Health must take reasonable steps to check that it is up-to-date, complete, relevant and not misleading. This will often depend on how long it has been since the information was collected originally.

What is 'reasonable' depends on the proposed use for the information and its impact on the service

user. The more important or sensitive the use, which is to be made of the information, the more careful we need to be to make sure it is accurate and make any necessary additions or changes.

The People and Capability team will ensure employee information is checked for accuracy at least every two years.

Service user information will be checked for accuracy on an ongoing basis by employees when maintaining a service user database or service user's Service Plan (and this will occur on at least an annual basis).

8. USING PERSONAL INFORMATION

Access Community Health will only use personal information for the purpose/s that it was obtained. This includes uses that are directly related to the purpose for obtaining the personal information.

For example, information obtained for care and treatment may also be used for administrative purposes related to that care and treatment.

In limited circumstances, personal information may be used in a way which was not anticipated when it was obtained. For example, relevant personal 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. 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) or for the conduct of proceedings.

When considering whether or not information may be used in a way that is not connected to the original purpose it was collected for, Access Community Health employees must consult the Privacy Officer for advice and guidance. The Privacy Officer will be responsible for deciding whether or not information may be used in a different way to that originally anticipated when collected.

9. DISCLOSING PERSONAL INFORMATION

Disclosure of personal information that Access Community Health holds can raise some challenging questions where Access Community Health:

- has to disclose;
- wants to disclose; and/or
- has been asked to disclose.

In all circumstances where Access Community Health discloses personal and/or health information to any party other than the individual concerned, the disclosure will be marked "Strictly Confidential".

9.1. Dealing with situations where we must disclose

Any law that authorizes or requires personal information to be made available takes precedence over the Privacy Act and Health Information Privacy Code. If a law requires disclosure, the relevant information must be made available.

When Access Community Health is asked to disclose information under some legal authority, employees should refer the request to the Privacy Officer. Access Community Health's policy in this situation is to ask to see the authority (e.g. a Police warrant) or to determine what that authority is (e.g. what legislation the authority is claimed under), in order to assess whether there are restrictions on what information can be provided, and how the information is obtained, provided or used.

The Privacy Officer will also consider whether the individual who the information relates to should be told that their personal information has been requested and disclosed. The disclosure will also be noted on the relevant file and the individual may be made aware of the disclosure if they later access their own personal information.

Health and Disability Commissioner Act 1994, section 62

The Health and Disability Commissioner can require Access Community Health (as a service provider) to make information available for an investigation conducted by the Commissioner.
The Privacy Officer or Chief Operating Officer will be responsible for determining the release of this information when requested.

The Privacy Act, sections 86-87

The Office of the Privacy Commissioner can require Access Community Health to disclose information for investigations conducted under the Privacy Act.

The Privacy Officer will be responsible for determining the release of this information when requested.

Search warrant

Access Community Health must disclose relevant information in response to a court order such as a search warrant.

The Privacy Officer will be responsible for determining the release of this information when requested.

9.2. Dealing with situations where we want to disclose

In a situation where we want to disclose information to a third party, but this disclosure does not appear to fall under the original purpose/s the information was collected for, then we must find a statutory provision that allows it (either in the Privacy Act, Code or some other legislation). Some of these provisions are detailed below. ***In these circumstances, the Privacy Officer should be consulted prior to the disclosure of personal information.***

Oranga Tamariki Act 1989, sections 15-16

Under these sections anyone who believes a child or young person is at risk of some harm, ill-treatment, abuse, neglect or deprivation can report the matter to a social worker or the Police. These provisions permit, rather than require, the disclosure. They also protect disclosers from civil, criminal or disciplinary proceedings if the disclosure is made in good faith.

Health Information Privacy Code, Rule 11

Rule 11 prohibits disclosure unless one of the specific exceptions applies, or there is some other law allowing disclosure. However, disclosure under the Code is discretionary. This means that even where Rule 11 allows a disclosure, the disclosure does not have to be made.

The main exceptions in rule 11 that will apply to Access Community Health are set out below.

Rule 11(1) of the Code allows disclosure where the disclosure:

- is to the individual concerned or his or her "representative" where the individual is dead or is unable to exercise his or her rights under the Code.
- is authorised by the individual concerned or his or her "representative" where the individual is dead or is unable to exercise his or her rights under the Code.
- is to an individual's principal caregiver and relates to the individual's release, or imminent release from compulsory status under the Mental Health (Compulsory Assessment and Treatment) Act 1992. "Principal caregiver" means the friend or family member who is most concerned with oversight of the individual's care and welfare. This exception allows some disclosures, but the most useful and flexible method of ensuring caregivers have the information they need is to make a clear discharge plan that addresses the issue of disclosure to family.

Right 4(5) of the Code of Health and Disability Services Consumers' Rights gives consumers the right to co-operation among providers to ensure quality and continuity of services. Cooperation may require sharing information between providers where necessary for treatment. So this sharing would be a purpose for having the information. That purpose should be communicated to the service user when the information is collected.

Disclosure where a service user is unconscious, not competent, or has refused to give authorisation

In cases where a service user is unconscious, not competent, or has refused to give authorisation for disclosure, Rule 11(2) of the Code allows disclosure where:

- **The information is disclosed by a health practitioner to a person closely associated with the service user.** 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. In these cases, the disclosure must be in line with recognised practice, and not be contrary to the express request (i.e. veto) of the service user or their representative (where the service user can't give a decision).

- **The disclosure is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of the individual or another individual.** The disclosure must be to someone who can do something to lessen the risk such as the Police or an at-risk associate of the individual. Only the information necessary to achieve that goal should be given.
- **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.** For instance, Access Community Health may wish to disclose to the Police or to a public sector agency such as the Inland Revenue Department, Ministry of Social Development or Immigration New Zealand. It is important to check with the Privacy Officer before disclosing information on this basis to ensure that we do not breach privilege; and/or that it is appropriate to disclose the information in the context in which is requested.
- **The information is disclosed because Access Community Health believes the individual is (or is likely to become) dependent on a controlled drug, prescription medicine or restricted medicine.** This type of disclosure has to be to the Medical Officer of Health under the Misuse of Drugs Act or the Medicines Act. This provision does not cover disclosure of information about drug seekers to other health agencies directly.
- **The disclosure is in accordance with an authorisation granted under section 30 of the Privacy Act.** The Privacy Commissioner can permit some one-off disclosures in the public interest that would otherwise breach the Code's Rule 11. This would be arranged via the Privacy Officer.
- **The information is disclosed for research and statistical purposes,** will not be published in a form which could identify anyone and ethical committee approval has been obtained if necessary.

9.3. Dealing with situations where we have been asked to disclose

Access Community Health may need to respond to unexpected requests for information. For example, because:

- the Police are investigating a crime;
- the media are following up a story;
- a DHB wants clinical information to assess the effectiveness of a clinical programme it is funding;
- a social worker is investigating a case of suspected abuse; or
- a family wants information about a relative who is receiving treatment.

Health Act 1956, section 22F

Section 22F allows health practitioners to obtain health information from other health practitioners – for instance, if a service user transfers to a new clinic and his or her notes are needed from the old clinic for the service user's medical history. Caregivers and representatives can also use it to obtain information. Requests for this information would be actioned/approved by a clinician or appropriate Regional Manager and ***Privacy Officer should always be consulted prior to making a decision under section 22F.***

As part of our Informed Consent Process a service user may give consent to personal information being shared with their advocate/agent/next of kin.

Under section 22F health information must (with some exceptions) be disclosed, on request, to the individual, individual's representative or any person providing health or disability services to the individual (including caregivers).

However, a section 22F request may be refused if Access Community Health believes, on reasonable grounds, that the service user does not want the information to be disclosed to the representative, caregiver or service provider. Talking to the service user about the request is not legally required, but is usually good practice.

Where the service user's representative has made the request, Access Community Health may also refuse the request if the disclosure would be contrary to the service user's interests or one of the withholding grounds in the Privacy Act (sections 49-53) would apply if the request had been made by the service user (discussed below). If the exceptions do apply, the agency may still disclose the information if it wants to.

If none of these exceptions apply, the information must be disclosed in accordance with the request. ***The Privacy Officer should always be consulted prior to making a decision under section 22F.***

Guardians of children under 16 may consent on their child's behalf to medical, dental and surgical procedures under the Care of Children Act 2004. The Code of Health and Disability Services Consumers' Rights gives consumers the right to be fully informed when giving consent. This should be considered when dealing with requests by guardians for personal information if they have been asked to consent to a child's treatment.

Health Act 1956, section 22C

Under this section, Access Community Health is allowed to disclose health information to specific categories of people, on request, if that information is required for those people to carry out their powers, duties and/or functions as set out in section 22C (2).

Section 22C allows information to be disclosed in response to a request. It does not allow information to be volunteered without a request. Also, the disclosure is always discretionary.

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

- police officers;
- medical officers of penal institutions;
- probation officers;
- CYF social workers and care and protection coordinators.

Information may also be disclosed to the employees of a DHB. 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. The Privacy Officer should always be consulted prior to making a decision under section 22C.

Health Act 1956, section 22D

The Minister of Health can require any District Health Board to disclose information about the condition or treatment of, or health or disability services provided to, any person.

The Minister can require disclosure only for the purpose of obtaining statistics for health purposes or for the purposes of advancing health knowledge, health education or health research.

Information which would identify the person concerned may only be provided under this section if the person concerned, or their representative consents to the disclosure or the identifying information is essential for the purposes for which the information is sought.

Official Information Act 1982

Access Community Health is not subject to the Official Information Act (OIA) as this legislation applies only to public sector agencies. However, this legislation is relevant to Access Community Health given that many of our funders and contracting partners (including the Ministry of Health, DHBs, and ACC) are subject to this legislation. So, any personal information we provide to the public agency will become subject to the OIA. For this reason, care must be taken when disclosing information to these public sector agencies to ensure that the particular information is identified as personal information and protected accordingly.

9.4. Non-Work Communications and Social Media

Access Community Health employees will not disclose personal information relating to colleagues, service users or any other third parties connected to their job in any communications with any parties outside of their role. This includes making any disclosures via social media channels such as Facebook, Twitter, Instagram and/or Snap Chat (this relates to both public and private channels). It also includes communications via personal devices such as mobile phones and tablets.

10. DEALING WITH REQUESTS FOR DISCLOSURE

If Access Community Health receives a request involving the disclosure of information, the first step is to determine whether the request was made by the individual concerned, their agent or by someone who may fall within a certain category which may permit disclosure (e.g. representative, funder, another service provider).

11. SPECIAL ISSUES RELATING TO DISCLOSURE

11.1. Disclosure to family, caregivers and friends

The safest way to disclose information to people who are close to a service user is always to get permission from that service user for the disclosure. However that is not always possible or practical. Rule 11 of the Code allows disclosure to family, partners or friends in specific circumstances, even without the authorisation of the service user. For example, where a health practitioner isn't able to get someone's permission for disclosure, then information about them may be disclosed to the service user's:

- principal caregiver
- near relative; or
- nominated contact person.

The disclosure must be in line with recognised professional practice and, importantly, the service user can veto the disclosure.

11.2. Dealing with service user concerns over disclosure

Sometimes service users do not want their families or friends to be given information about their illnesses or treatment. They may not want information to be passed to other health practitioners who will be monitoring their treatment and recovery. These types of concerns might be dealt with in a number of ways discussed further below.

Where disclosure is a purpose

Access Community Health may consider a purpose for obtaining health information is to pass on necessary information about care of the service user to caregivers or other people who should be aware of certain aspects of care, such as medication requirements. The Code permits this disclosure where it is one of the purposes for which the information was obtained, and where the service user has been informed about this purpose at the time of collection of the information.

Developing a plan at the outset, with the service user's involvement, enables desired disclosures to be discussed. It will reduce the need to approach the service user later for an authorisation to disclose information.

Where an individual vetos disclosure

If information was obtained for a particular purpose, including disclosure to a caregiver, and the service user was aware of this purpose at the time the information was collected, the disclosure may be made despite a service user's later veto although ethics would need to be considered. Where the purposes do not include disclosure of certain information, Access Community Health must consider other options including whether one of the exceptions to the Code's Rule 11 applies.

Discussion with the service user is often the best starting point. Where appropriate, if we consider disclosure to a caregiver or family member is not in the individual's best interests (perhaps because of family dynamics or because of potential harm to the therapeutic relationship), the person requesting information should be advised that the decision not to disclose has been made on clinical grounds.

Disclosure to prevent a threat or for the maintenance of the law

There may be a compelling interest in disclosure, perhaps to avert a suicide or to warn that a service user in the community poses a health or safety risk. If there is a serious threat to public health or safety, or the life or health of any individual, the Code will permit disclosure of relevant information to an appropriate person who can act to prevent or lessen the threat.

First, decide if it is desirable or practicable to get the individual's authorisation. If so, talk to the person and seek their permission for the disclosure. If not, consider whether:

- there is a serious threat to public health or public safety or to someone's life or health; and
- it is necessary to disclose health information to lessen or prevent the threat.

The information should be disclosed only to a person or agency who can act to lessen or avert the threat. And remember that it may not be necessary to disclose all of the information to avert the threat.

Only necessary information should be disclosed. ***Where possible, consult the Privacy Officer in the first instance.***

There may also be a compelling interest in disclosure of certain information to the Police or some other public sector agency with a function of maintaining a law. First, decide if it is desirable or practicable to get the individual's authorisation. If so, talk to the person and seek their permission for the disclosure. If not, consider whether it is necessary to disclose health information to avoid prejudice to the maintenance of the law. The disclosure needs to be made to a public sector agency which maintains the law in question. It may not be necessary to disclose all of the information to avoid the prejudice. Only as much information as is necessary to do so should be disclosed.

12. REQUESTS TO ACCESS PERSONAL INFORMATION

All individuals have a right to access personal information about themselves no matter where it is held.

A request cannot be refused on the basis that the individual does not "own" the records or that the information "belongs" to the agency.

People do not have to explain why they want to see their personal information. However, their reasons for requesting personal information may sometimes become relevant when balancing different privacy interests. For instance, where there is mixed information about two people, Access Community Health will have to decide whether releasing information about the other person would

be an unwarranted breach of their privacy.

Information "held in the mind" can also be subject to an access request, provided it is readily retrievable. People cannot necessarily be expected to remember in detail events which occurred a number of years ago. But they may remember that they had a particular conversation, or that a specific issue was discussed at a meeting a few weeks or months ago, and this can be revealed.

The Act and Code gives individuals a right to access information (which will often mean getting a copy of that information) but not to demand original documents.

The Health (Retention of Health Information) Regulations 1996 allows disposal of health information by giving the notes to the individual concerned. If an individual requests old information that Access Community Health no longer wishes to keep and does not have to keep (because more than 10 years have elapsed since the last treatment episode), Access Community Health can consider giving the individual the records.

12.1. Requests by employees

Requests made by employees to access the personal information the employer holds about them will be dealt with by their manager with the assistance of the People and Capability team.

12.2. Requests by parents and guardians

Parents and guardians of a child under 16 years are the child's representative under the Code and section 22F of the Health Act.

Under the Code and section 22F of the Health Act, parents and guardians have a limited right of access to health information of their children under the age of 16. In the case of very young children there would seldom be reason to withhold the information from a parent as a representative of the child.

This sort of request under section 22F may be refused where:

- it would be contrary to the interests of the child or young person to disclose
- the child or young person does not or would not wish the information to be disclosed
- withholding grounds in sections 49-53 of the Privacy Act would have applied, had the request been made by the person concerned.

One parent or guardian of the child cannot veto the release of information to another parent or guardian under the Code or following a section 22F request by another parent or guardian. The Privacy Officer should be consulted where there is any dissent relating to the release of information between parents and guardians.

12.3. Responding to requests for personal health information by the person concerned

Access Community Health must make a decision on an access request as soon as reasonably practicable, and within 20 working days (at most) after receiving the request.

Access can be granted by:

- allowing inspection of the documents;
- providing a copy of the documents;
- hearing or viewing audio or video tape recordings;
- supplying transcripts;
- supplying a summary of the information; and/or
- an oral explanation.

Access should be granted in the manner preferred by the requester, unless it would impair efficient administration (e.g. it might be very expensive or problematic). Where an individual is given access to personal information following a request for the information, he or she must be informed that they can request correction of the personal information.

Access Community Health must ensure that any personal information intended for an individual is received only by the individual or that individual's authorised agent.

People may ask an agent to make a request on their behalf. Access Community Health should therefore ensure that any agent for someone else has a written authorisation (preferable) or is otherwise authorised to make the request (e.g. the agent may be a lawyer, who has confirmed that he or she has an authorisation).

12.4. Reasons to withhold personal information

The reasons available to refuse a request for access to personal information held about that individual are contained in sections 49-53 of the Privacy Act. These reasons include that:

- it would create a serious threat to the health, safety or life of any individual, or to public health or safety;
- it would create a significant likelihood of serious harassment to an individual;
- it would cause significant distress to a victim of an offence;
- it would disclose a trade secret or unreasonably prejudice the commercial position of the agency or someone else who has supplied or is subject to the relevant personal information;
- the disclosure of the information would involve the unwarranted disclosure of the affairs of another individual or of a deceased individual;

- the disclosure of the information or of information identifying the person who supplied it, being evaluative material, would breach an express or implied promise of confidentiality;
- after consultation undertaken (where practicable) by or on behalf of the agency with an individual's medical practitioner, the agency is satisfied that the information relates to that individual; and the disclosure of the information (being information that relates to the physical or mental health of the individual who requested it) would be likely to prejudice the physical or mental health of that individual;
- in the case of an individual under the age of 16, the disclosure of that information would be contrary to that individual's interests;
- the disclosure of that information (being information in respect of an individual who has been convicted of an offence or is or has been detained in custody) would be likely to prejudice the safe custody or the rehabilitation of that individual;
- the disclosure of the information would breach legal professional privilege; or
- the request is frivolous or vexatious, or the information requested is trivial.

In addition, Access Community Health may refuse an access request if:

- the information requested is not readily retrievable; or
- the information requested does not exist or cannot be found; or
- the information requested is not held by us and the person dealing with the request has no grounds for believing that the information is either held by another agency; or connected more closely with the functions or activities of another agency.

Under sections 24 and 29 of the Privacy Act, requested personal information may also be withheld if a provision in another statute imposes a prohibition or restriction in relation to the availability of that personal information.

If Access Community Health refuses access to information, it must tell the requester:

- the reason for the refusal;
- that they have a right to make a complaint to the Privacy Commissioner and to seek an investigation and review of the refusal; and
- If the individual requests it, the grounds in support of the reason, unless giving those grounds would itself prejudice the interests protected under sections 49-53 of the Privacy Act.

13. REQUESTS FOR CORRECTION OF PERSONAL INFORMATION HELD

People have a right to ask for their personal information to be corrected. Access Community Health does not have to make the correction if it believes it is not appropriate to make the correction requested.

If Access Community Health does not agree to make the correction sought it must, if requested, take reasonable steps to attach a statement of the correction that the requester wants. If reasonably practicable the statement must be attached so that it will always be read with the disputed information.

The requester should provide the statement of correction in his or her own words. However, Access Community Health should provide reasonable assistance and it might be helpful in the circumstances for Access Community Health to prepare a draft statement, setting out the requester's objections, for his or her approval.

Access Community Health should take steps to correct personal information where necessary. If personal information has not been directly obtained from the individual concerned, it may be best to verify the accuracy of it with that person. If an agency suspects the information is not accurate, it must be checked before being used.

When steps are taken to correct information or attach a statement, Access Community Health must then take reasonable steps to inform everyone who has previously received the information (this could be by way of an email, a telephone call or a letter). The more significant the potential consequences of the information going uncorrected, the more important it is for the agency to let relevant people know about the correction.

14. DISCLOSING INFORMATION OVERSEAS

Access Community Health may disclose personal information to a foreign person or entity who is subject to comparable privacy safeguards, or when the disclosure is authorised by the person to whom the information relates (per Privacy Principle 12). Access Community Health will ensure that appropriate contractual arrangements are in place with any offshore parties in respect of privacy safeguards before disclosing any personal information.

Using offshore cloud providers or other agents to store or process data is not treated as a disclosure under Principle 12, so long as the agent or cloud provider is not using that information for their own purposes.

15. HANDLING PRIVACY COMPLAINTS AND INADVERTENT DISCLOSURES/ BREACHES

Managing a privacy complaint

1. Any complaints relating to privacy should be referred to the Privacy Officer immediately. He/she will decide whether or not a case can be handled individually or escalated for an inquiry process. It is expected that the relevant Manager will work alongside the Privacy Officer to work through any complaints received or breaches occurring.

2. The Privacy Officer will determine who is to be contacted following a privacy complaint or breach notice. This may include the relevant funder/s (most funding service agreements require immediate notification in the event of a privacy disclosure or serious complaint), the person whose information it relates to, and senior management.

3. When a complaint of a breach of the Act or Code is received it must be managed as set out below:

   (a) The complaint must be acknowledged in writing in 5 working days of receipt, unless it has been resolved to the satisfaction of the complainant within that period; and

   (b) The complainant must be informed of Access Community Health's complaint procedure; and

   (c) The complaint and the actions taken by Access Community Health must be documented; and

   (d) Within 10 working days of acknowledging the complaint, Access Community Health must:

      – decide whether it accepts the complaint is justified or not; and

      – if it decides more time is required to investigate the complaint, determine how much additional time is needed; and

      – if the additional time exceeds 20 working days, inform the complainant of that and of the reasons for it; and

   (e) As soon as practicable after an agency decides whether or not it accepts that a complaint is justified, it must inform the individual of:

      – the reasons for the decision; and

      – any actions proposed to be taken; and

      – any appeal procedure available; and

      – the right to complain to the Office of the Privacy Commissioner.

4. The Privacy Officer may establish a Privacy Review Committee (consisting of 3 impartial members of the Senior Leadership Team or delegates) called together for each inquiry arising. The Privacy Officer will always be a member, and convenor, unless he/she is involved or implicated in the case/complaint themselves.

5. The Privacy Officer will develop a Terms of Reference (including timelines) for any Privacy Review Committee (PRC) inquiry.

6. All parties involved in a PRC inquiry will receive a copy of the Terms of Reference and the associated summary report. All steps in a PRC inquiry will be treated as strictly confidential.

7. The Privacy Officer will update the Chief Executive regarding any privacy complaints occurring as part of regular reporting.

8. At the end of a PRC inquiry, the Privacy Officer will draft a Privacy Report noting the PRC's findings and recommendations – to be considered by the Chief Executive.

Managing an inadvertent privacy disclosure

1. An inadvertent privacy disclosure (or breach where harm has occurred) is the result of unauthorised access to or collection, use or disclosure of, personal information. All inadvertent privacy disclosures or breaches (actual or potential) will be reported to the Privacy Officer without delay.

2. The four key steps to consider when responding to an inadvertent privacy disclosure or breach (or suspected breach) are:

   (a) breach containment and preliminary assessment;

   (b) evaluation of the risks associated with the breach;

   (c) notification (including consideration of whether or not the breach is notifiable); and

   (d) prevention.

3. Steps 1, 2 and 3 should be undertaken either simultaneously or in quick succession. In particular, in most cases, anyone whose personal information has been disclosed should be notified as soon as possible, with an apology and steps outlined as to what is being done about it. 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.

   NOTE: *A breach of privacy by an employee of Access Community Health may result in informal action (such as restriction of email functionality, undertaking further training or any other appropriate sanction) or it may result in formal action (such as investigation and disciplinary outcomes).*

4. The Privacy Officer is responsible for managing Access Community Health's response to any inadvertent privacy disclosures or breaches (alongside the relevant manager), and updating the relevant senior management as part of regular reporting.

5. The Privacy Officer will consider whether or not to engage with the Office of the Privacy Commissioner when investigating and managing a suspected privacy breach, including assessing whether it is a Notifiable Privacy Breach (see below).

Notifiable Privacy Breaches

It is mandatory for agencies to notify the Office of the Privacy Commissioner (OPC) if a privacy breach has caused, or is likely to cause, serious harm. Serious harm is a very high threshold to be met.

It is also necessary for an agency to notify an affected individual as soon as practicable after becoming aware that a notifiable privacy breach has occurred. Public notice may also need to be considered.

In any case where it appears that a privacy breach with the potential for causing any form of harm has occurred, the Privacy Officer must be notified immediately and they will manage the next steps to be taken.

What is serious harm?

The unwanted sharing, exposure or loss of access to people's personal information may cause individuals (or groups) serious harm. Some information is more sensitive than others and therefore more likely to cause people serious harm.

Examples of serious harm include:

- Physical harm or intimidation
- Financial fraud including unauthorised credit card transactions or credit fraud
- Family violence
- Psychological, or emotional harm

Assessment on whether to notify

The following is a guide developed by the OPC to help agencies to assess whether or not a privacy breach may involve serious harm and therefore require notification:

1. Does it involve personal information? (yes/no)

2. How sensitive is the information involved? (e.g. sensitive; likely sensitive; not likely sensitive)

   Sensitive information can be, for example, about someone's health, political or religious beliefs, or financial information. Context is important. Information that is not sensitive in one situation might be very sensitive in another

3. Recipient: who has obtained, or may obtain, the personal information? (e.g. someone likely to cause harm; someone unlikely to cause harm; someone uncooperative; someone unknown)

4. Types of harm: what types of harm may be caused by individuals affected by the breach?

   E.g. – discriminatory; emotional; financial; employment; identity theft; loss of access to information; loss of opportunity; physical; reputational; threats of harm

5. For each type of harm, rate the likely impact on affected individuals (low/high)

6. Likelihood of harm: how likely is it that someone will be harmed by this breach? (e.g. harm has already occurred; likely; unlikely)

7. Attempts to reduce harm: what steps have been taken to reduce the harm, or further harm, from this breach? (e.g. information was recovered and not accessed; the device was wiped remotely and the information not accessed; the problem that caused this breach has been fixed; the recipient(s) of the information were contacted; or other steps)

8. Security measures: are there security measures in place that protect the information from being accessed? (yes/no)

Based on the answers to the questions above, assess and weigh up whether the actual or potential harm that is likely to occur meets the 'serious' threshold.

GLOSSARY

Act means the Privacy Act 2020.

Code means the Health Information Privacy Code 2020.

Employee means all current and former employees of the organisation (including temporary employees and contractors, and subsidiaries), and any person who is involved in the delivery of services Access Community Health provides (including Board members).

Health practitioner has the meaning given to it by the Health Practitioners Competence Assurance Act 2003. Not every health professional is a "health practitioner". If an individual provides health services, even where the particular discipline is not listed in the Health Practitioners Competence Assurance Act 2003, that individual will still be a "health agency" for the purposes of the Privacy Act 2020.

Health information is:

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

f) incidental to, the provision of any health service or disability service to that individual.

Information in this document includes personal information and health information.

Personal information is information about an identifiable individual.

Principal caregiver means the person responsible for a service user's care (usually a family member).

Privacy Officer is the appointed person within the organisation who has responsibility for this policy and Access Community Health's obligations under the Privacy Act 2020.

Representative, in relation to an individual, means:

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).

Service User means a person receiving services from the organisation (e.g. a client or service user of Access Community Health or a subsidiary).