Information safeguards

"They look after my personal information."

Intent

We take the job of safeguarding personal information seriously. We monitor risks to data security and implement measures to address these risks in line with good practice.

This policy prescribes minimum operational and electronic safeguards. We will vary these safeguards to ensure we respond to new and emerging risks. For information safeguards when working remotely, including when working from home, see Remote working information security. For Protection of privacy see here.

Definitions

"Information" in this policy involves personal and organisational information.

"Personal information" is information relating to an identifiable person including hard copy, digital and electronic information. It includes health information.

"Organisational information" refers to information about our business affairs whether stored in hard copy, digitally or electronically.

"Unique identifiers" are individual numbers, references, or other forms of identification allocated to people by organisations eg driver's licence and passport numbers; the NHI number assigned by Ministry of Health for health services.

Requirements

Privacy and data security training

Kaimahi will be trained in privacy and data security good practice.

The Office of the Privacy Commissioner's 'Privacy ABC' or an equivalent level of training should be completed at least every two years https://elearning.privacy.org.nz/

Operational safeguards

The following safeguards will be adhered to:

- information will only be accessed if authorised and as-necessary (based on role and responsibilities)
- personal information will not be discussed or stored in public areas
- paper records will be scanned and stored electronically. If this is not reasonably practicable, paper records containing personal information will be kept in a secure place (eg locked filing cabinet)
- records relating to a rangatahi known or related to a staff member/kaimahi will be kept confidential from the staff member concerned
- when kaimahi/others leave the organisation, their email address will be disabled and their emails and calendar appointments archived
- rangatahi, /staff and others' personal information will not be kept on personal laptops or home PC
- when sharing information, all due care will be taken to transmit the information securely:
    - check the physical and electronic address of the recipient before sending

    - send the information to a named authorised person in the safest and most confidential way eg use a tracked courier for physical transfer of a person's record - copy or original.
- if it is necessary to remove personal or confidential information from the premises, the information must be kept secure (eg personal information carried in a locked bag).

Accessing personal information other than for authorised and professional purposes will be treated as a disciplinary matter.

Electronic record safeguards

Personal information will be held and stored electronically with appropriate safeguards in place, including:

- password/login system for secure access
- a screen saver programme to minimise risk of unauthorised access to files
- regular back-up of records with recovery of information from the back-up tested regularly
- where possible, workstations and computers are positioned to avoid personal information on screens being seen by unauthorised people
- terms and conditions of software, including cloud-based CMS, are complied with
- client data is not left on an unattended screen or left open when other people are present
- anti-virus software is installed and run regularly.

Unique Identifiers

People will only be assigned a unique identifier or reference if necessary (for protection purposes or for our efficient functioning). Reasonable care will be taken to protect unique identifiers from misuse.

No one will be asked to disclose an identifier that was assigned by another agency unless we are wanting it for the original reason it was assigned.

Risk management

Privacy risks will be monitored and regularly reviewed. Safeguards for new and emerging risks will be implemented that are proportionate to the level of risk we identify.

Risks and measures taken to address risks will be recorded in the organisational risk register.

The Privacy breach policy will be applied to prevent and respond to a breach.

Safe disposal of personal information

Personal information will be securely disposed of once the purpose for which we collected it no longer applies and provided we are not required by law to keep it (eg health & disability requirements; wages records) or the person/whānau to whom it relates does not want it.

Reasonable care will be taken to safeguard privacy during the destruction process. Records on our computer hardware and any backup of the records will be wiped in such a way as to be unable to be reconstructed in any way.

Virus protection

All due care must be taken to avoid the risk of computer virus transmission:

- avoid opening 'executable' files (those ending in .exe) and other files (.com, .vbs etc.) that are known to transmit viruses via attachments to emails
- avoid opening email if in doubt about the contents
- disable macros in Office and Excel
- ensure that anti-virus software is run and updated at least weekly.

Helpful links

Back to Protection of Privacy

Breach of privacy

Health Information Privacy Code 2020

Cybersecurity and risk management. Issues for consideration at board level.

CERTNZ, Critical Controls 2022

Tutaki Client Recordkeeping

Review

Date: October 2020

Next review: by September 2022