RMG
Rotorua Medical Group

Privacy Policy

Purpose

Rotorua Medical Group acknowledges the importance of protecting patients’ health information and will endeavour to ensures it’s security at all times.

This policy therefore, outlines information in relation to the Privacy Act, which promotes and protects the privacy of information collected from and about an individual and the Health Information Privacy Code, which was established specifically for the management of information relating to health and disability support services such as general practice.

Scope

All staff must comply with the following rules when collecting, using, storing or disclosing information about patients’ health or the treatment that they are receiving.

The privacy officer is the practice manager (https://www.privacy.org.nz/tools/online-privacy-training-free/) has completed extensive privacy training, including Privacy 101 and Health 101, and provided in house training for other staff members. Records of this are held by the practice manager.

Collecting health information

When you collect health information from patients you must:

- only collect the information for the purpose of treating the patient or for some other legal purpose;
- collect the information directly from the patient unless he/she has consented to you collecting the information from someone else or one of the other exceptions to this rule applies; and
- let the patient know why you are collecting the information, who will have access to the information and that the patient is entitled to access and correct the information. You will not need to tell patients this if you have collected the same type of information from them before.

Using health information

Before using patients’ health information, you must do what you can to make sure that the information is accurate and up to date. The steps that you will need to take will vary depending on how old the information is and the risk of relying on inaccurate information in the circumstances.

You must only use patients’ health information for the purpose for which you have collected the information unless the patient has consented to you using the information for another purpose, or one of the other exceptions in the Health Information Privacy Code applies. You must consult our practice’s Privacy Officer before using a patient’s health information without the patient’s consent.

Storing health information

To ensure that the health information that our practice holds is stored securely so that it cannot be accessed or used by unauthorised people you should follow this process:

- All hard copy notes are to be filed into the practice hard file for patient notes. The patients name and file number is to be recorded on the front of the file and on the spine.
- At time of writing this policy notes are not destroyed.
- All patient records are kept and maintained on Indici Patient Management System (PMS). This is routinely backed up via our support at the PHO, RAPHS. Staff have unique Identification and passwords to ensure only verified staff members are able to access the PMS.
- When you transfer patients' health information to someone else, you must do what you can to prevent unauthorised people from accessing or using the information.
- Our practice can keep patients' health information for as long as we need the information to treat patients and must keep patients' health information for a minimum of 10 years from the date that treatment was last provided.
- Our practice must destroy patients' health information in a way that ensures the confidentially of the information. ***ALL PATIENT HEALTH INFORMATION SHOULD BE PLACED IN THE DESTRUCTION BIN.***

Patients disclosing health information

- Patients are entitled to ask our practice to confirm whether we hold information about them and to access the information unless we have lawful reasons for withholding the information.
- Patients are also entitled to ask our practice to correct the information that we hold about them.
- You must assist patients who ask to access their health information.

Disclosing health information

You must not disclose a patient's health information without his/her consent (or the consent of his/her representative) unless you reasonably believe that it is not possible for you to get the patient's consent and:

- the disclosure is for the purposes of the patient's treatment (e.g. a referral);
- the disclosure is to the patient's caregiver and the patient hasn't objected to the disclosure;
- it is necessary for you to disclose the information to prevent a serious and immediate threat to the patient or another person's life or health;
- the disclosure is made for the purposes of a criminal proceeding;
- the patient is, or is likely to become dependent on a drug that you need to report under the Misuse of Drugs Act or the Medicines Act;
- the disclosure is to a social worker or the police and concerns suspected child abuse;
- the disclosure is made by a doctor to the Director of Land Transport Safety and concerns the patient's ability to drive safely.

Doc Date: Dec 2022
Due Date: Dec2024 Signed: CRGoldsmith (PM)

There are other situations where disclosure without consent may be justified, such as disclosing information to agencies such as Oranga Tamariki and the Police. You must discuss any proposed disclosure with our practice's Privacy Officer before disclosing the information.

You must consult with our practice's Privacy Officer before disclosing a patient's health information without his/her consent. The Privacy Officer.

Please contact our practice's Privacy Officer if you have any queries about this policy.

Checking that health information is accurate and up to date

Steps that you should take to make sure that your patients' health information is accurate and up to date include:

- checking how old the information is;
- confirming with the patient that the information remains accurate;
- if necessary, updating the information (e.g. by carrying out new tests).

Transferring patients' health information securely

Whenever you send patients' health information to another person or agency, you should make sure that the information is sent securely and confidentially by:

- Putting the information in a courier bag or envelope stamped "private and confidential" and "for addressee only";
- Keep a record of all files transferred (including electronic patient notes). Note the date sent, patient name or file number, method sent by, and to whom they were addressed;
- Only sending patients' health information by **email**, or electronically, if you are sure that the email address or fax number that you are sending the information to is correct and that the information will not be able to be accessed by people who are not authorised to receive it.

Paper Records

Paper Records – use within the practice

- Where a patient record is in a consultation room, but not actively being viewed during a consultation, it should be closed, covered or placed in a position to avoid incidental disclosure
- Patient records must be covered, so that no personal identifiers are visible when moving records within the practice

Paper Records – transported in personal vehicles

- Patient records must be in a closed bag/container ensuring personal identifiers are not visible
- Practitioners should minimize the time patient records are left unattended in a vehicle

Paper Records – storage

- Patient records are to be stored away from unauthorized individuals in a secure area

- Access is managed in a coordinated manner

  a) Individuals with the authority to access the secured area are identified. This includes all employees
  b) Confidentiality agreements for after hour's staff/contractors are completed.

Electronic health records

- Passwords access to the PMS system is central to security. Each user must have a unique login name and password. The latter must be at least medium strength, that is an alphanumeric combination at least 8 characters.

- On screen patient data should not be able to be read by unauthorised persons (those who do not have access rights to patient notes). This is particularly important in areas of the practice where such screens might be visible to the wider public other than authorised staff or the patient concerned.

- There is evidence (contract with RAPHS) that appropriate firewall and other internet security (e.g. antivirus) measures are in place.

- The practice has a clear policy on the disposal of computer equipment containing patient data that prevents the data being recovered by unauthorised persons. (This only applies to any computers which store information outside of the remote access to RAPHS where all patient information is stored.)

New Privacy 2020 law changes

The most significant change for general practice are **notifiable privacy breaches**. Under the new Act, if an organization has a privacy breach that causes harm, they will need to notify the Privacy Commissioner and affected people. It will be an offence to fail to notify the Privacy Commission of a notifiable privacy breach.

- Staff are to notify the practice's Privacy Officer asap
- Go to the online site https://privacy.org.nz/responsibilities/privacy-breaches/responding-to-privacy-breaches/ and go through the 4 key steps : Contain ,Assess ,Notify , Prevent
- Under the changes to the Privacy Act 2020, an organisation will have to notify the Privacy Commissioner of a privacy breach, if it poses a risk of serious harm to individuals. If you are unsure as to whether the breach is a serious one, our NotifyUs tool will help you make that assessment. You can also contact the Privacy office and discuss the matter with them .

Doc Date: Dec 2022
Due Date: Dec2024 Signed: CRGoldsmith (PM)

Resources

Office of the Privacy Commissioner | Health Information Privacy Code 2020 access to the 5 Health Information Privacy Code 2020 factsheets

Office of the Privacy Commissioner | Responding to privacy breaches
Health Information Privacy Code 1994
Healthy Practice (MAS)
RAPHS Information Security Framework
RAPHS Policies and Procedures Manual IS Section

Doc Date: Dec 2022
Due Date: Dec2024

Signed: CRGoldsmith (PM)