Privacy Policy for Rolleston Central Health

1 SUMMARY

The confidentiality, collection, storage, disclosure, transfer, disposal and protection of information relating to patients and activity of this medical centre is of significant importance requiring clear policy and procedural understanding.

2 POLICY STATEMENT

2.1 Purpose

The needs and rights of patients in respect to personal information will be protected when this policy is adhered to.

This policy outlines the privacy protocols that will be followed by staff working in this practice and to comply with the:

- Privacy Act 2020
- Health Information Privacy Code 2020 (HIPC).
- Health (Retention of Health Information) Regulations 1996

This policy also addresses the requirements of the Foundation Standard supporting the patient experience and equity meeting their needs and rights.

2.2 Background

Personal information is any information which tells us something about a specific individual. The information does not need to name the individual, as long as they are identifiable in other ways, like through their home address. The Privacy Act is concerned with the content of personal information, rather than the specific form that content is in. This means that all sorts of things can contain personal information, including notes, emails, recordings, photos and scans, whether they are in hard copy or electronic form.

At the core of the Privacy Act 2020 are 13 information privacy principles that set out how agencies may collect, store, use and disclose personal information.

- Principles 1, 2, 3, & 4 govern how you can collect personal information. This includes when you can collect it, where you can collect it from, and how you can collect it.
- Principles five, six, and seven govern how you store personal information. People have a right to access and seek correction to their personal information.
- Principles 8, 9, 10,11 & 12 govern how you use and share personal information. Make sure information is accurate, and you use and share it appropriately.
- Principle 13 governs how "unique identifiers" - such as IRD numbers, bank client numbers, driver's licence and passport numbers - can be used.

  For more information see: https://privacy.org.nz/privacy-act-2020/privacy-principles

The Health Information Privacy Code builds upon the Privacy Principles and provides a minimum set of standards in relation to the handling of health information.

2.3 Scope

This policy applies to all staff engaged in any activity carried out at this practice including those not directly employed by the practice e.g., Mental Health professionals, laboratory personnel etc.

2.4 Responsibilities

All staff are responsible for ensuring this policy is followed.

The designated Privacy Officer for Rolleston Central Health is Phil Batchelor.

The Privacy Officer is responsible for ensuring that the practice and its entire staff comply with this policy, the Privacy Act and the HIPC.

The Privacy Officer shall ensure that all members of staff have received training on the management of Health information. The Privacy Officer will also ensure that all staff who have access to patient information have signed confidentiality agreements – see appendix 1.

The Privacy Officer will monitor privacy issues and in conjunction with the complaints officer will manage privacy complaints.

2.5 Definitions & Abbreviations

HIPC	Health Information Privacy Code 2020
Personal Information	Any information about a living, identifiable individual. This includes (but is not limited to) people's names, contact details, health records, financial records, and unique identifiers like NHIs: anything that you can look at and say "this is about an identifiable person"
Health Information	Health information about an identifiable individual, including information about health and disabilities, medical history, any health or disability service provided, information collected while services are provided-for example details for billing purposes.
Privacy Breach	(1) any unauthorised or accidental access to or disclosure, alteration, loss or destruction of Personal Information; or (2) any action that prevents the Practice from accessing the Personal Information on either a temporary or permanent basis; and (3) includes any of the things listed above, whether or not it: (i) was caused by a person inside or outside the Practice; or (ii) is attributable in whole or in part to any action by the Practice; or (iii) is ongoing or a one-off event.

2.6 Related Policies

- Implementation of the Code of Health and Disability Service Consumers' rights
- Complaints Policy
- Security of Electronic Health Information Policy

3 POLICY DETAIL AND PROCEDURES

Confidentiality

All staff engaged by Rolleston Central Health who have access to patient's personal and health information will sign a confidentiality agreement confirming they have read and understand this policy and the requirements of the Privacy Act and HIPC in respect to patient personal information. See appendix 1 for sample Confidentiality Agreement. The confidentiality agreement will be read in conjunction with privacy and confidentiality in employment contracts and agreements, and any staff Code of Conduct, as applicable.

Collecting health Information

Rolleston Central Health will only collect information that is relevant and required for the purpose of treating an individual, monitoring quality of care provided or administrative purposes.

Wherever possible the information will be obtained directly from the patient. Exceptions include when someone else is authorised to provide the information (such authorisation ideally being in writing) or when the patient is unable to do so.

Patients will be advised that the information is being collected, who will have access to it, why the information is being collected, the consequences of not providing the information and that they have a right to correct the information. The details for this could be provided orally, in a brochure, letter or poster or could be included in the enrolment form. We will utilise the Pegasus PHO "Enrolling with a Primary Health Organisation – Health Information Privacy Statement" as the basis for this advice.

Privacy protections

We will ensure the environments and devices that we use to collect information reduce the risk of unintended disclosure of personal and health information, this would include (but is not limited to):

- Steps to provide privacy in reception areas for times when personal information is collected. This may include use of background music or television in waiting areas or a private location to help protect personal information.
- Where Clinicians undertake video/telephone consultations they will:
    - Ensure they are in a private setting where they cannot be overheard.
    - confirm the patient is in a private setting where the consultation cannot be viewed or overheard.
    - Advise the patient if the consultation is being recorded along with explaining the purpose for recording the consultation.
- Medical imaging will not be recorded on personal mobile devices or cameras. Rolleston Central Health provides a dedicated cell phone to be used for all medical imaging. Images are downloaded and saved to patient's clinical notes immediately and deleted from the device/camera.

Security of Information

Health information will be stored for at least 10 years after the last contact with that patient[1]

Health information will be stored securely with safeguards to prevent access by unauthorised people or its loss.

- All computers will have individual user passwords for access to programmes or files containing identifiable personal information or clinical records.
- Staff will access records in accordance with their duties and role-based access to programmes may apply.
- Time activated screen locking will be in place requiring staff to log on after 2 hours of inactivity.
- Filing cabinets, rooms and other areas used to store personal information will be locked when they are unattended.
- Back up of computer systems will be completed each working day with a restore test being performed once every 6 months to ensure the validity of the backup.
- When required, the destruction of private information will be in a secure manner such as shredder, burning or by an approved document destruction contractor.

Access to personal Information

All patients can access, and correct personal and health information held about themselves. This includes former patients where information is being retained under the requirements of the Health (Retention of Health Information) Regulations 1996. No fee will be charged for a person wishing to access their health information/medical records. A request can be made verbally or in writing. (It may be useful to have the request in writing for clarity and scoping of the information sought).

Disclosure

Health Information will not be disclosed without the authorisation of the patient unless:

- It is to the individual patient concerned (or their authorised representative).
- There is reasonable belief that it is not possible to get such consent and is for the purpose of treatment.
- Disclosure is one of the reasons for which the information was obtained.
- Disclosure is required to prevent serious and immediate harm to the individual.
- It is to appropriate agencies for suspected child abuse.

[1] as required under the Health (Retention of Health Information) Regulations 1996

- Disclosure is to the Land Transport Authority when there are serious concerns about an individual's ability to drive without endangering themselves or others.
- It is for the purposes of a criminal proceeding.
- The individual is dependent on or seeking a drug (Misuse of Drugs Act 1975 and section 49a of Medicines Act 1981). A warning could be displayed in the waiting area advising that information about suspected drug seekers may be disclosed.
- Disclosure to the Police under section 92 of the Arms Act 1983, relating to the use or possession of firearms.
- Disclosure is authorised or required under any other legislation.

Breach Notification

Where any member of the Practice becomes aware of a potential privacy breach, they will respond as quickly as possible to initially contain the breach and notify the Privacy Officer. As a practice we will utilise the Privacy Commissioners 4 step process to help minimise any harm caused to the affected person/people and our practice.

There are four key steps in dealing with a privacy breach:

1. Contain
2. Assess
3. Notify
4. Prevent

We will complete the first three steps either at the same time or in quick succession. We will use step four to come up with longer-term solutions and prevention strategies.

We will evaluate a risk of harm to the patient or their Whanau that may result from any privacy breach. We will consider each incident on a case-by-case basis and think about:

- The risk of harm to people affected.
- Whether there's a risk of identity theft or fraud.
- Whether there's there a risk of physical harm.
- Whether there's a risk of humiliation, loss of dignity, or damage to the person's reputation or relationships. For example, if the lost information includes mental health, medical, or disciplinary records.
- What affected people can do to avoid or minimise possible harm, e.g., change a password.
- Whether we have any legal or contractual obligations.

We will use all facts we have about the situation (and the guidance available from the Privacy Commissioner's Office) to decide whether we will notify the people affected. Where the breach has caused serious harm, or is likely to do so, we will:

1. Notify the Patient directly.
2. Use the Privacy Commissioners "NotifyUs" tool to report or update a breach.

   https://www.privacy.org.nz/responsibilities/privacy-breaches/notify-us/

Resources: https://www.privacy.org.nz/responsibilities/privacy-breaches/responding-to-privacy-breaches/

Transfer of health Information

Medical records and other information will only be transferred to another health provider when a written request has been received. If an individual verbally requests a transfer of their records, they must sign a form to acknowledge the request. All requests will be scanned into the medical record of that individual.

The transfer should be completed in no more than 10 working days.

Request will be discussed with the appropriate doctor to ascertain whether copies of paper notes are to be retained (noting the requirement to then store the information for up to 10 years).

When medical records are being requested for a new patient, the patient will indicate this on the practice's enrolment form.

In managing patient records, we will also comply with the requirements of the Medical Council's document: *Managing Patient Records* (October 2019)

4 REFERENCES

- Privacy Act 2020
- Health information Privacy Code 2020
- Privacy Commissioner. (2013). *Information Privacy Principles*. Retrieved from Privacy Commissioner: http://www.privacy.org.nz
- Health (Retention of Health Information) Regulations 1996
- *Managing Patient Records,* Medical Council of New Zealand, October 2019. available at: https://www.mcnz.org.nz/assets/standards/ca6c11b3cd/Maintenance-patient-records.pdf

Authorised by: Dr Philip Schroeder
Date: May 2024 **For two yearly review**

Staff Confidentiality Agreement

Staff working at this medical centre will be exposed to personal and health information of patients which is protected in terms of the Privacy Act 2020 and the Health Information Privacy Code 2020

I, _____, have read and understand the provisions of Rolleston Central Health Privacy Policy and understand that whilst working here I need to ensure that all personal and health information is kept confidential, secure and managed in line with the policy.

I agree that I will only access information which is required as part of my duties.

I have been made aware of the requirements of the Privacy Act 2020 and the Health Information Privacy Code 2020 (HIPC) as it relates to my role at this practice. I understand that my obligation with respect to the confidentiality of personal and health information will endure after I have finished working at this practice.

……
Name

……..
Signature

……...
Date