



Privacy Policy

At Functional Again we are committed to safeguarding your privacy. This privacy policy and agreement (this "**Privacy Policy**") covers how we collect and use information in our electronic medical records and practice management software systems that can be used to identify you and that was created, used or disclosed in the course of providing a health care service (your "**Protected Information**"), which includes information that you provide or access via the patient portal at <https://functionalagain.practicebetter.io> (the "**Patient Portal**").

In this policy, "you" and "your" refer to a user of the Patient Portal, patient, or other person with Protected Information on file with Functional Again. "Functional Again", "we", "our" and "us" refer to Functional Again Ltd and its subsidiaries and affiliates.

Please read this policy carefully. By checking the box or otherwise signifying the acceptance of this privacy policy, you are acknowledging that you have read it, understand it and are agreeing to be legally bound by the terms provided here.

The information we collect

We collect Protected Information in the form of (1) registration information that you provide in order to enrol as a patient or use the patient portal (your "**Personal Information**"); (2) information that is created, used, or disclosed in the course of providing healthcare services to you, which we file in your medical record electronically and/or on paper (your "**Protected Health Information**"); and (3) the financial records, such as billing or insurance information, records of payments and balance statements related to our provision of health care services to you (your "**Billing Information**"). We do not collect and/or retain any more protected information than reasonably necessary to provide our services, operate our electronic medical record and the patient portal, and respond to your requests.

By law, you have the right to access and amend your medical records. We own original copies of any records created by us or shared with us, which we maintain in accordance with New Zealand Law. We may provide you with access to your Protected Information via electronic or paper records created from the patient portal at our discretion as a convenience to you. We may ask for Protected Information concerning family members or others for whom you are authorised to act as a personal representative. We use this information to create and gather medical records for these people, and will use and disclose this information in the same manner as we use and disclose your Protected Information.

Our use of Your Protected Information

We will not share your protected information with any third party, other than as expressly disclosed in this policy. In general, we will use your Protected Information as necessary to provide you with care, respond to your requests and maintain our records and the patient portal. We will use your billing information to obtain payment for the services that we provide to you.

We will use and disclose your protected information in accordance with the Health Information Privacy Code 2020 (HIPC). The practice complies with the HIPC when storing, correcting or destroying your protected information.

Printed information about our Privacy Policy is available on request and information is displayed in our reception. All our staff will have training to ensure adherence with Privacy legislation.

Disclosure of health information

We do not disclose a patient's health information without his/her consent (or the consent of his/her representative) unless we reasonably believe that it is not possible for us 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 us 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 we 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.

By submitting Protected Information to us that you received from hospitals, physicians, or other records owners, you are consenting to the disclosure of this information to our staff for use in your treatment programs.

Disposal of information

The practice's policy is to follow the guidelines of the HIPC (Health Information Privacy Code Fact Sheet 5).

In summary;

- * the practice may dispose of information at 10 years and 1 day following the date of the last consultation, if the designated patient's practitioner is satisfied this is reasonable.
- * Should your practitioner die or cease to practice, the clinic will enquire whether you would prefer to 1) transfer to new clinician, 2) have your records returned to you or 3) have your records held in trust until one of the two options above can take place.

When information is no longer needed any paper with patient identifiable information will be shredded. Computers that contain health information that are no being used or are for patients that are leaving the practice will have the data rendered irretrievable.

Anonymous aggregate information

"Aggregate Information" is information that does not identify you, such as statistical information and analyses concerning the use of our services, the number of customers registered in our Electronic Medical Record (EMR), usage data for the Patient Portal, aggregated information about health statistics, treatments, conditions or similar aggregated healthcare information, or other aggregated information that is not personally-identifiable.

We may use or disclose Aggregate Information in order to undertake or commission statistical and other summary analyses of (i) the general behaviour and characteristics of users participating in our services (ii) the effect of our services on the behaviour of our patients, and (iii) the general characteristics of visitors to our website or the Patient Portal and participants in our services. We may share these analyses and Aggregate Information with third parties.

Aggregate Information provided to third parties will not allow anyone to identify you, or determine anything personal about you. We may collect Aggregate Information through features of the software that supports our services, through cookies, and through other means in the future as described below.

IP Addresses

We do not receive and record information in our server logs from your browser, including your IP address, your computer's name, the type and version of your web browser, referrer addresses and other generally accepted log information. We may record page views, and other general statistical and tracking information, which will be aggregated with that of other users but this will not be disclosed to third party.

Cookies

A cookie is a small amount of data, which often includes an anonymous unique identifier, which is sent to your browser from a website's computers and is stored on your computer's hard drive. Cookies can be used to provide you with a tailored user experience and to make it easier for you to use a website upon a future visit. Our websites use cookies.

Privacy Protection for Children

We will not provide access to the Protected Information of anyone under the age of 18 (a "Minor Dependent") via the Patient Portal except:

- * We may share Protected Information in communications between a parent or legal guardian and Functional Again Ltd. regarding a Minor Dependent's care, to the extent permitted by the Health Information Privacy Code 2020 (HIPC) and other applicable laws protecting the privacy of the Minor Dependent;
- * Personal Information of a Minor Dependent will be linked to a parent's or guardian's Patient Portal account;
- * Where a third party is responsible for billing and payment, Billing Information BUT NOT related Protected Health Information of a Minor Dependent may be shared with the third party payor.

In general, the Protected Information of a Minor Dependent will be disclosed to a parent or guardian in accordance with the HIPC Health Information Privacy Policy.

Health Records Maintenance

In the course of maintaining your records, our staff, employees and technical/maintenance contractors (the "Contractor") may have limited or full access to your protected information. Such individuals may include a technician or service provider that provides us with the technology, services, and/or content related to (i) enhancing operation and maintenance of the Patient Portal or our electronic records, (ii) responding to and sending electronic mail in support of help requests or (iii) providing other functions necessary to our business. Access to your Protected Information by a Contractor is limited to the information reasonably necessary for that Contractor to perform his or her limited functions for us. We also contractually require each Contractor to protect the privacy of your information consistent with this Privacy Policy.

Condition-specific content

Periodically, we may send you news, bulletins, educational materials, marketing materials, or other information based on your Protected Health Information, e.g. targeted to your specific health condition(s). If we choose to send such communications, you will have the ability to opt-out of receiving them, as further provided below.

Opt Out

If we choose to send you bulletins, updates, or other unsolicited, marketing-related communications, we will provide you with the ability to opt-out of receiving such communications.

However, you may not opt-out of formal notices concerning (i) the operation of our EMR (Electronic Medical Record) or the Patient Portal, or (ii) legal and other related notices concerning your relationship to us. Nor may you opt-out of being provided with content passively via internet that you choose to access.

Security

Security measures are in place to protect the loss and misuse of your Protected Information.

SECURITY MEASURES

The Patient Portal uses TLS 1.2 encryption technology (an industry-standard technology) to prevent phishing and to safeguard your Protected Information whenever it is transferred between servers and AES-256 bit encryption when storing your data on their servers. Practice Better have HIPAA Business Associate Agreements and GDPR Data Processing Agreements with all third parties which store and process data on their behalf.

Our security systems are structured to prevent unauthorised third parties from accessing your Protected Information. However, we do not warrant as fail-proof the security of your Protected Information. Due to the nature of internet communications and evolving technologies, we cannot provide, and we explicitly disclaim, assurance that your Protected Information will remain free from loss or misuse by third parties who, despite our efforts, obtain unauthorised access.

NOTICE OF SECURITY INCIDENT

If we detect or become aware of any unauthorised access to your Protected Information, we will notify you and/or the Secretary of Health and Human Services in accordance with New Zealand law.

CHANGES TO THIS PRIVACY POLICY

We reserve the right to change this Privacy Policy at any time. If we make any changes to this Privacy Policy, you will be prompted to accept the revised Privacy Policy in order to continue using the Patient Portal. If we make any changes regarding disclosure of your Protected Information to third parties, we will attempt to contact you prior to the date that the modified policy is scheduled to take effect via your recorded email address on file.

EFFECTIVE DATE

The effective date of this Privacy Policy is January 29th, 2025.

I accept and agree to the terms of this Privacy Policy.

Please tick the box

☐

Patient Name :

Date :