

balance!

*Health Care*

# Balance! Health Care

## Privacy Policy

*PO Box 6024, Silverwater NSW 2128*

*Telephone: 1300 854 340*

*[www.balancehealthclinic.com.au](http://www.balancehealthclinic.com.au)*

# Balance! Healthcare privacy policy

Current as of: 1 January 2024

Balance! Springwood Family Practice

Balance! Edmonton Family Practice

Blackheath Family Medical Centre

## Introduction

This privacy policy is to provide information to you, our patient, on how your personal information (which includes your health information) is collected and used within our practice, and the circumstances in which we may share it with third parties.

## Why and when your consent is necessary

When you register as a patient of a doctor at our practice, you provide consent for your doctor to use the information you provide to manage your health care which may include using the information for the following purposes (including instructing the practice to use the information for the following purposes on your doctor's behalf):

- Collect, record and store my personal and health information that will form part of an individual computerised medical record.
- Issue reminders for specific health checks you may require, if any, as part of my consultation with my doctor and/or nurse.
- Provide you with health information updates, general medical updates and provide personal and health information to the relevant state and/or national recall reminder registers.
- Use personal and health information to undertake, however not limited to; administrative tasks involved in the running of the Practice, and for doctor, billing tasks which includes compliance with Medicare, Health Insurance Commission and other relevant Government agency requirements.

## What personal information does the doctor collect?

The information that is collected about you includes:

- names, date of birth, addresses, contact details
- medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors
- Medicare number (where available) for identification and claiming purposes
- healthcare identifiers
- health fund details.

## Dealing with us anonymously

You have the right to deal with the doctor anonymously or under a pseudonym unless it is impracticable for us to do so or unless we are required or authorised by law to only deal with identified individuals.

## How does your doctor collect your personal information?

Your doctor will collect your personal information:

1. When you make your first appointment our practice staff will collect your personal and demographic information via your registration.
2. During the course of providing medical services, we may collect further personal information. This may be collected through Electronic Transfer of Prescriptions (eTP), Electronic Transfer of Radiology, Electronic Transfer of Pathology, and information from your My Health Record/PCEHR system, through a Shared Health Summary or an Event Summary.
3. They may also collect your personal information when you visit our website, send us an email or SMS,

telephone us, make an online appointment or communicate with us using social media.

4. In some circumstances personal information may also be collected from other sources. Often this is because it is not practical or reasonable to collect it from you directly. This may include information from:
  - your guardian or responsible person
  - other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services and pathology and diagnostic imaging services
  - your health fund, Medicare, or the Department of Veteran's Affairs (as necessary).

## Who does your doctor share your personal information with?

The doctor sometimes shares your personal information:

- with third parties who work with the doctor for business purposes, such as accreditation agencies or information technology providers – these third parties are required to comply with APPs and this policy
- with other healthcare providers
- when it is required or authorised by law (eg court subpoenas)
- when it is necessary to lessen or prevent a serious threat to a patient's life, health or safety or public health or safety, or it is impractical to obtain the patient's consent
- to assist in locating a missing person
- to establish, exercise or defend an equitable claim
- for the purpose of confidential dispute resolution process
- when there is a statutory requirement to share certain personal information (eg some diseases require mandatory notification)
- To allow medical students and authorised staff to participate in medical training/teaching
- For the purposes of medical research and peer education only where de-identified information is used
- Follow up reminder/recall notices by letter or telephone (including contact via SMS to the provided mobile phone number) for treatment and preventative health care
- during the course of providing medical services, through Electronic Transfer of Prescriptions (eTP), Electronic Transfer of Radiology, Electronic Transfer of Pathology, and information from your My Health Record/PCEHR system, through a Shared Health Summary or an Event Summary.

Only people that need to access your information will be able to do so. Other than in the course of providing medical services or as otherwise described in this policy, the doctor will not share personal information with any third party without your consent.

We will not share your personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without your consent.

Your doctor will not use your personal information for marketing any of our goods or services directly to you without your express consent. If you do consent, you may opt-out of direct marketing at any time by notifying our practice in writing.

## How does the doctor store and protect your personal information?

The doctor holds personal information in our clinical software, which is entered either by direct entry or by electronically scanning paper documents into the patient file. Paper documents are securely destroyed once scanned to the clinical software. Your personal information may include as visual informations such as X-rays, CT scans, and occasionally photos we may take if agreed with you at the time.

The doctor stores all personal information securely. This is done in electronic format, in protected information systems. All passwords to this system are tightly controlled and our IT provider, Your IT, has signed a confidentiality agreement for their staff and contractors.

If the doctor receives unsolicited personal information about a patient from another health practitioner or practice, the doctor will hold such information for a period of four (4) weeks on the presumption that the patient will attend the practice for a consultation. If the patient does not attend the practice within four (4) weeks the unsolicited information about the patient will be securely destroyed.

## How does the doctor manage access to your My Health record?

The doctor holds personal information in our clinical software, a sub section of which is uploaded to My Health record on request. Only clinical staff have the ability to update your My Health record, and this will happen while you are in the consultation with the doctor or nurse.

Staff are trained when they start in our practice and we ensure staff are aware of the My Health Record and privacy obligations, and handle personal information in a consumer's My Health Record accordingly. This training is updated annually, and there is ad hoc training when there are changes to legislation or My Health Record system functionalities.

Our software provider has an audit trail, and at all times the practice is able to identify a person who requests access to a healthcare recipient's My Health Record and communicating the person's identity to the System Operator. The Manager accesses Audit logs and regularly monitors staff access to the My Health Record system. Audit logs record the user identity, date and time of access, whose My Health Record was accessed and the type of information that was accessed.

The practice has a password standard of 13 or more characters (using a combination letters, numbers and symbols) for all passwords that are used for access to the My Health Record system. If the passwords are compromised then the suspension of the user account will happen immediately.

## How does a doctor deal with notifiable data breaches?

A data breach will be a notifiable data breach where there is unauthorised access to, or unauthorised disclosure, or loss of, personal information held by the doctor and that you could conclude that there is a likely risk of serious harm as a result. This could include physical, psychological, emotional, economic and financial harm, and serious hard to reputation.

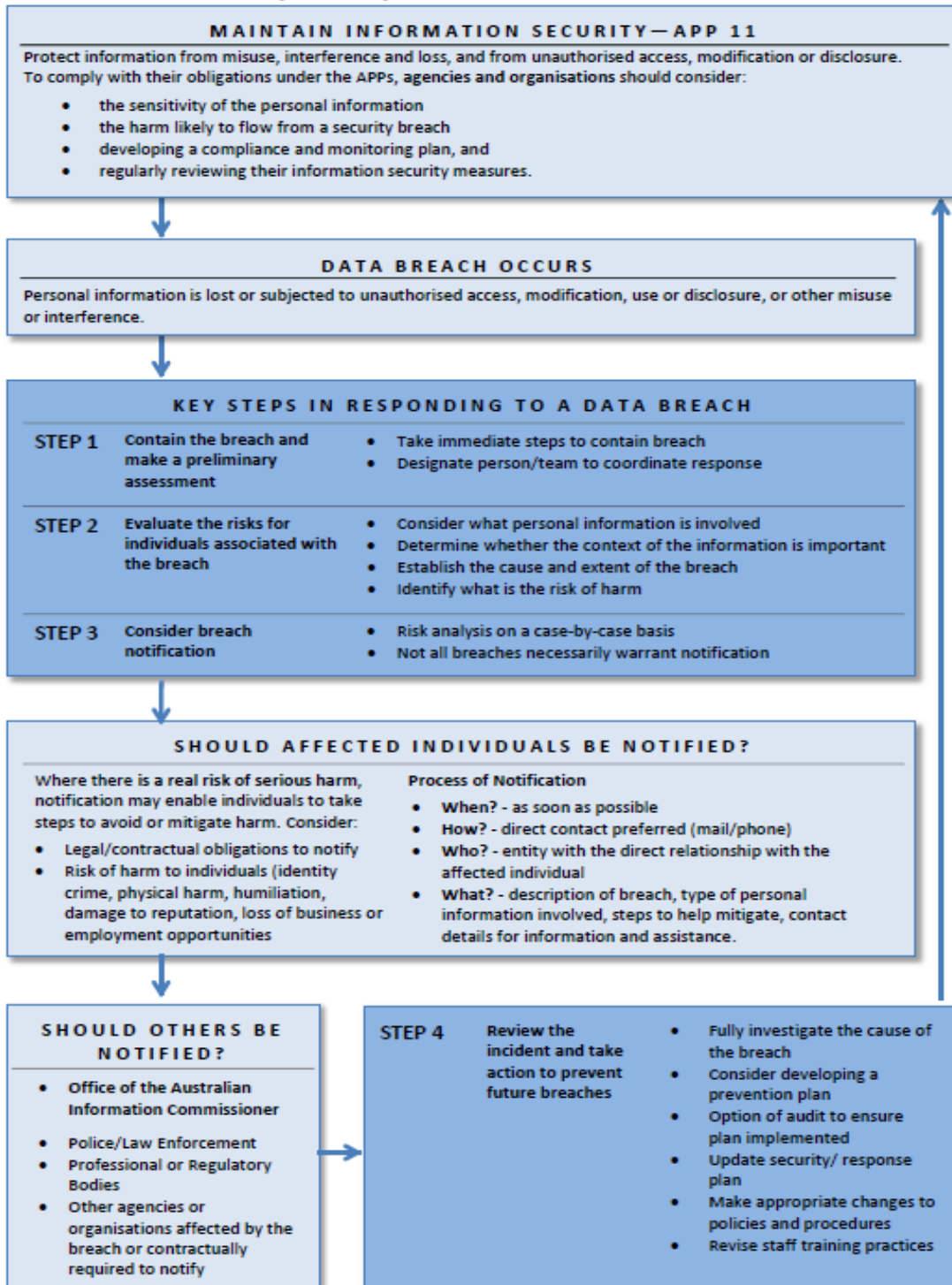
Breaches that are quickly rectified, so that you are not at risk of serious harm, do not require notification. Breaches that cannot be rectified must be notified to you and the Office of the Australian Information Commission. This information will include: the identify and contact details of the practice, a description of the data breach, the kind of information being the subject of the brief, and the proposed recommendations on any actions to be taken in response to the breach.

The chart below outlines our Data Breach Response Process<sup>1</sup>.

---

<sup>1</sup> Date Breach Information Guide: A Guide to Handling Personal Information Security Breaches.  
[www.oaic.gov.au/resources/agencies-and-organisations/guides/data-breach-notification-guide-august-2014.pdf](http://www.oaic.gov.au/resources/agencies-and-organisations/guides/data-breach-notification-guide-august-2014.pdf)

## Data breach response process



## How can you access and correct your personal information at our practice?

You have the right to request access to, and correction of, your personal information.

Your doctor acknowledges patients may request access to their medical records. We require you to put this request in writing (letter or email) and the practice will respond within 30 days. You may be charged \$20-\$40 for a copy for medical record.

The doctor will take reasonable steps to correct your personal information where the information is not accurate or up-to-date. From time-to-time, the practice will ask you on behalf of your doctor, to verify your personal information held by our practice is correct and up-to-date. You may also request that we correct or update your information, and you should make such requests in writing to the Practice Administration Manager

at your local practice or by emailing [kategunn@balancehealthclinic.com.au](mailto:kategunn@balancehealthclinic.com.au).

## How can you lodge a privacy related complaint, and how will the complaint be handled at our practice?

We take complaints and concerns regarding privacy seriously. You should express any privacy concerns you may have in writing. We will then attempt to resolve it in accordance with our resolution procedure. We will contact you within 30 days of receiving your complaint.

To make a complaint please contact Kate Gunn on 0411 466080 or email her on [kategunn@balancehealthclinic.com.au](mailto:kategunn@balancehealthclinic.com.au). You may also make your complaint in writing addressed to:

**Balance! Healthcare  
PO Box 6024  
Silverwater NSW 2128**

You may also contact the OAIC. Generally the OAIC will require you to give Balance! Healthcare time to respond, before they will investigate. For further information visit [www.oaic.gov.au](http://www.oaic.gov.au) or call the OAIC on 1300 336 002.

## Privacy and our website

Your doctor does not currently collect personal information via our website or Facebook page. If this changes in the future we will update this privacy policy.

## Policy review statement

This privacy policy will be reviewed regularly to ensure it is in accordance with any changes that may occur. We will notify your patients when we amend this policy by placing a sign on the front counter.