PRACTICE PRIVACY POLICY

Bulleen Plaza Medical Centre practice Privacy Policy Australian Privacy Principle's (APP's)

The Commonwealth Privacy Act was amended in 2012 and from March 2014 incorporates 13 Australian Privacy Principles (APP) that set out the rules for the handling of personal information in Australia.

From 12 March 2014, the Australian Privacy Principles (APPs) will replace the National Privacy Principles and Information Privacy Principles and will apply to organisations, and Australian Government (and Norfolk Island Government) agencies.

The Act will replace the existing nine Information Privacy Principles (IPPs) that apply to the public sector; the nine National Privacy Principles (NPPs) that apply to the private sector; along with 13 Australian Privacy Principles (APPs) that will apply to the public and private sector alike.

Health practitioners fall within the definition of an organisation that handles personal information so the APPs apply to them.

Personal information means information or an opinion – whether true or not – about an individual whose identity is apparent or can be reasonably ascertained.

In Victoria, health practitioners are also subject to the Health Records Act 2001 (Vic), which requires organisations dealing with health information to comply with the 11 Health Privacy Principles (HPPs).

The new APPs will apply in addition to the Victorian HPPs. The APPs are more similar to the existing HPPs than the federal principles they are replacing. This is good news for Victorian doctors because it means minimal changes will be required regarding the way health practitioners handle their patients' personal information. This document, commonly called a privacy policy, outlines how we handle personal information collected (including health information) and how we protect the security of this information. It must be made available to anyone who asks for it and patients are made aware of this.

The statement informs patients about how their health information will be used including other organisations to which the practice usually discloses patient health information and any law that requires the particular information to be collected.

Patient consent to the handling and sharing of patient health information should be provided at an early stage in the process of clinical care and patients should be made aware of the collection statement when giving consent to share health information.

In general, quality improvement or clinical audit activities for the purpose of seeking to improve the delivery of a particular treatment or service would be considered a directly related secondary purpose for information use or disclosure so we do not need to seek specific consent for this use of patients' health information, however we include information about quality improvement activities and clinical audits in the practice policy on managing health information.

We inform our patients about our practice's policies regarding the collection and management of their personal health information via:

- Brochures in the waiting area
- Our patient information sheet
- New patient forms- "Consent to share information " Verbally if appropriate

Introduction

Our practice is committed to best practice in relation to the management of information we collect.

This practice has developed a policy to protect patient privacy in compliance with privacy legislation. Our policy is to inform you of:

- the kinds of personal information that we collect and hold

- how we collect and hold personal information;
- the purposes for which we collect, hold, use and disclose personal information;
- how you may access your personal information and seek the correction of that information;
- how you may complain about a breach of the Australian Privacy Principles and how we will deal with such a complaint;
- whether we are likely to disclose personal information to overseas recipients

What kinds of personal information do we collect?

The type of information we may collect and hold includes personal information about

- Your name, address, date of birth, email and contact details
- Medicare number
- Your health information and other sensitive information

How do we collect and hold personal information?

We will generally collect personal information:

- from you directly when you provide your details to us;
- from a person responsible for you
- from third parties where the Privacy Act or other law allows it

Why do we collect, hold, use and disclose personal information?

In general, we may collect, hold, use and disclose your personal information for the following purposes:

- to provide health services to you
- to communicate with you
- to comply with our legal obligations which may include mandatory notification of communicable diseases
- to help us manage our accounts and administrative services.

Are we likely to disclose your personal information overseas?

We may disclose your personal information to the following overseas recipients: ·any practice or individual who assist us in providing services (such as where you have come from overseas and had your health record transferred from overseas or have treatment continuing from an overseas provider)

- anyone else to whom you authorise us to disclose it and ·anyone else where authorised by law

How can you access and correct your personal information?

Subject to the exceptions set out in the Privacy Act, you may seek access to and correction of the personal information which we hold about you in accordance with our access policy. If a fee is charged for providing access, you will be advised of the cost in advance.

How can you make a privacy related complaint?

We will take reasonable steps to protect the security of your information and comply with our legal obligations.

Our staff are trained and required to respect your privacy. We take reasonable steps to protect information held from misuse and loss and from unauthorised access, modification or disclosure.

If you have any questions about privacy related issues or wish to complain about a breach of the Australian Privacy Principles or the handling of your personal information by us, please contact our Privacy Officer- practice Manager
The contact person in this practice is Ellen Assad
You may lodge your complaint in writing. Any complaint will be investigated by the Privacy Officer and you will be notified of the making of a decision in relation to your complaint as soon as is practicable after it has been made, usually within 30 days
Prior to a patient signing consent to the release of their health information patients are made aware they can request a full copy of our privacy policy and collection statement.
Patient consent for the transfer of health information to other providers or agencies is obtained on the first visit.
Once signed this form is scanned into the patient's record and its completion noted.

Date of policy: 08.02.20

Name of practice: Bulleen Plaza Medical Centre

Purpose

To ensure patients who receive care from the practice are comfortable in entrusting their health information to the practice. This policy provides information to patients as to how their personal information (which includes their health information) is collected and used within the practice, and the circumstances in which we may disclose it to third parties.

Related standards

RACGP Compliance indicators for the Australian Privacy Principles: an addendum to the computer and information security standards (Second edition).

Background and rationale

The APP provides a privacy protection framework that supports the rights and obligations of collecting, holding, using, accessing and correcting personal information. The APP consist of 13 principle-based laws
and apply equally to paper-based and digital environments. The APP complement the long-standing general practice obligation to manage personal information in a regulated, open and transparent manner.
This policy will guide practice staff in meeting these legal obligations. It also details to patients how the practice uses their personal information. The policy must be made available to patients upon request.

Practice procedure

The practice will:

- provide a copy of this policy upon request
- ensure staff comply with the APP and deal appropriately with inquiries or concerns
- take such steps as are reasonable in the circumstances to implement practices, procedures and systems to ensure compliance with the APP and deal with inquiries or complaints
- collect personal information for the primary purpose of managing a patient's healthcare and for financial claims and payments.

Staff responsibility

The practice's staff will take reasonable steps to ensure patients understand:

- what information has been and is being collected
- why the information is being collected, and whether this is due to a legal requirement •how the information will be used or disclosed

- why and when their consent is necessary
- the practice's procedures for access and correction of information, and responding to complaints of information breaches, including by providing this policy.

Patient consent

The practice will only interpret and apply a patient's consent for the primary purpose for which it was provided. The practice staff must seek additional consent from the patient if the personal information collected may be used for any other purpose

Collection of information

The practice will need to collect personal information as a provision of clinical services to a patient at the practice. Collected personal information will include patients':

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

A patient's personal information may be held at the practice in various forms:

- as paper records
- as electronic records
- as visual – x-rays, CT scans, videos and photos
- as audio recordings.

A copy of our practice privacy policy is located at reception and is available to patients upon request.

The practice features the following collection statement on each 'New Patient' registration form:

Bulleen Plaza Medical Centre located at 103 Manningham Rd, Bulleen VIC 3105 collects your personal details and health information to ensure we deliver the best possible healthcare service. Patients are entitled to access their information at any stage by contacting the practice or their GP. Your health information may be disclosed to other organisations over the course of your treatment and these instances will be discussed with you if required. Failure to provide accurate and comprehensive information could negatively affect your healthcare. If you have any concerns regarding your privacy, please contact the practice.

Prior to a patient signing consent to the release of their health information patients are made aware they can request a full copy of our privacy policy and collection statement.

Patient consent for the transfer of health information to other providers or agencies is obtained via a signed transfer form, which is then incorporated into the patient medical record.

Documents which contain patient health information sent to other health care providers, such as referrals, are discussed with patients prior to their distribution. All requests for access to health information by patients are documented and incorporated into the medical record.

All new patients' signed registration forms are scanned into their medical record/stored in their medical file.

The practice's procedure for collecting personal information is set out below.

- practice staff collect patients' personal and demographic information via registration when patients present to the practice for the first time. Patients are encouraged to pay attention to the collection statement attached to/within the form and information about the management of collected information and patient privacy.
- During the course of providing medical services, the practice's healthcare practitioners will consequently collect further personal information.
- Personal information may also be collected from the patient's guardian or responsible person (where practicable and necessary), or from any other involved healthcare specialists.

The practice holds all personal information securely, whether in electronic format, in protected information systems or in hard copy format in a secured environment.

Use and disclosure of information

Personal information will only be used for the purpose of providing medical services and for claims and payments, unless otherwise consented to. Some disclosure may occur to third parties engaged by or for the practice for business purposes, such as accreditation or for the provision of information technology. These third parties are required to comply with this policy.

The practice will inform the patient where there is a statutory requirement to disclose certain personal information (for example, some diseases require mandatory notification).

The practice will not disclose personal information to any third party other than in the course of providing medical services, without full disclosure to the patient or the recipient, the reason for the information transfer and full consent from the patient.

The practice will not disclose personal information to anyone outside Australia without need and without patient consent.

Exceptions to disclose without patient consent are where the information is:

- required by law
- 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 a confidential dispute resolution process

The practice will not use any personal information in relation to direct marketing to a patient without that patient's express consent. Patients may opt out of direct marketing at any time by notifying the practice in a letter or email.

The practice evaluates all unsolicited information it receives to decide if it should be kept, acted on or destroyed.

Access, corrections and privacy concerns

The practice acknowledges patients may request access to their medical records. Patients are encouraged to make this request in writing to the practice manager. Under law you have a right to access personal information we hold about you. Please contact our practice manager for more information on our Access to Medical Records Policy.

You will be required to put this request in writing to the practice Manager or email ellenassad@gmail.com and he will respond within 30 days. The practice 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 patients to verify that the personal information held by the practice is correct and up to date. Patients may also request the practice corrects or updates their information, and patients should make such requests in writing.
The practice takes complaints and concerns about the privacy of patients' personal information seriously.
Patients should express any privacy concerns in writing. The practice will then attempt to resolve it in accordance with its complaint resolution procedure.

Confidentiality and Privacy of Health Information:

This practice is bound by the Commonwealth Privacy Act – Privacy Amendment (Private Sector) Act 2000 and also complies with the Victorian Health Records Act 2001 and from 12 March 2014, the Australian Privacy Principles (APPs) will replace the National Privacy Principles and Information Privacy Principles and will apply to organisations, and Australian Government (and Norfolk Island Government) agencies.
Every effort is made within the practice to ensure that privacy is a top priority, both within the consulting area and the waiting room.
This practice has the ability to screen off the practice staff if on the telephone. There is a television in the waiting room and this helps to mask conversations.
The maintenance of privacy requires that any information regarding individual patients, including staff members who may be patients, may not be disclosed either verbally, in writing, in electronic form, by copying either at the practice or outside it, during or outside work hours, except for strictly authorised use within the patient care context at the practice or as legally directed.
There are no degrees of privacy. All patient information must be considered private and confidential, even that which is seen or heard and therefore is not to be disclosed to family, friends, staff or others without the patient's approval. Any information given to unauthorised personnel will result in disciplinary action and possible dismissal.
Each staff member is bound by his/her privacy agreement which is signed upon commencement of employment at this practice.

SUMMARY OF AUSTRALIAN PRIVACY

PRINCIPLES (APPS)

APP 1 OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

The practice must have an up to date and available privacy policy that covers specified information. The privacy policy must be made available to patients free of charge.

APP 2 ANONYMITY AND PSEUDONYMITY

Individuals must have the option of not identifying themselves, or using a pseudonym, unless impracticable or unlawful.

APP 3 COLLECTION OF SOLICITED INFORMATION

Sensitive information (including health information) must only be collected:

- with consent from the individual (or authorised guardian); and
- where reasonably necessary for the functions and activities of the practice

  (that is, the provision of health services).

Information should only be collected from the patient unless it is impracticable to do so.

Example: Information about a patient's family member is collected while taking a history. This is acceptable if the information is reasonably necessary to treat the patient.

APP 4 DEALING WITH UNSOLICITED INFORMATION

Where an entity receives personal information it did not solicit, it must determine whether the information could have been collected under APP 3. If not, the information must be de-identified or destroyed.

APP 5 NOTIFICATION OF COLLECTION OF PERSONAL INFORMATION

Individuals must be made aware of the nature of the personal information the practice collects. This includes information on:

- accessing and amending medical records
- how to make a complaint
- whether information will be used for direct marketing or disclosed to overseas recipients.

The practice's privacy and patient consent documents should cover these points.

APP 6 USE AND DISCLOSURE OF PERSONAL INFORMATION

Information collected by the practice must only be used for a primary purpose or a secondary purpose directly related to the primary purpose, and only where the patient has provided consent to the use or disclosure.

A 'primary purpose' is the reason the information was collected (for example, for the provision of health care)

A 'secondary purpose' is a purpose ancillary but closely related to the primary purpose. For example, using patient details for billing purposes, or disclosing patient details to a specialist for referral.

Disclosure may also be required by law, including where there is a:

- warrant from Police to access medical records
- subpoena to produce document or give evidence
- obligation of mandatory notification of child abuse or notifiable disease.

Use or disclosure for a secondary purpose is also lawful in 'permitted general situations', without consent of the patient. The most relevant of these include

- where necessary to lessen or prevent a serious threat to the life, health or safety of an individual or the public and it is unreasonable/impracticable to obtain the patient's consent. The threat need not be 'imminent' but it must be 'serious'.
- in instances of suspected or actual unlawful activity or serious misconduct that relates to the practice's functions and use or disclosure is necessary to take appropriate action.
- to locate a missing person – if the practice has a reasonable belief that the use or disclosure of personal information is reasonably necessary to locate a missing person. Example: medical records indicate a 17 yr old male who has been reported missing was proposing to travel interstate to meet a girl he met on facebook.
- to defend or establish a legal or equitable claim.
- to lawyers or insurers in response to complaints or claims.

- for confidential mediation/ADR processes – practices have the right to use or disclose patient information during a confidential alternative dispute resolution process such as mediation.

There are 3 ‘permitted health situations’ where a practice can use or disclose health or genetic information for a ‘secondary purpose’. These are:
Research- if relevant to public health or safety and it is impracticable to obtain a patient’s consent. The research must be conducted in accordance with research guidelines and the practice must reasonably believe that the information will not be further disclosed by the recipient.

APP 7 DIRECT MARKETING

The practice must not use personal information for direct marketing unless the individual has given specific consent for this to occur.
Direct marketing involves the use of personal information to communicate with an individual to promote goods and services.
Example: sending patients an SMS offering discounted services at the practice is direct marketing and not permitted. Direct marketing is permitted where an individual would have a reasonable expectation that this would occur and they can easily ‘opt out’.

APP 8 CROSS BORDER DISCLOSURE OF PERSONAL INFORMATION

If the practice is going to send personal information overseas, it must take reasonable steps to ensure the overseas recipient will not breach the APPs. There are exceptions where the overseas recipient has a similar enforceable law in place or the patient has consented after being expressly informed that information will be sent overseas.

- Prevention of a serious threat to the life, safety or health of a genetic relative. Example: a daughter may request access to her mother and grandmother’s medical records to determine the nature of their disease.
- Responsible person/Guardian – where a patient is either physically or mentally incapable of giving consent, a practice may disclose information to a responsible person or guardian where the disclosure is necessary to provide appropriate care or treatment to the patient or for ‘compassionate reasons’. The disclosure must not be contrary to the wishes of the patient and limited to the extent necessary for care or compassion.

Example: having a contract with an overseas cloud service provider that requires compliance with APPs.

APP 9 USE OF GOVERNMENT IDENTIFIERS

The practice must not adopt, use or disclose a government related identifier unless:

- the adoption, use or disclosure is required or authorised by law it is reasonably necessary to verify the identify of the individual.
- It is reasonably necessary to fulfil the obligations to a Commonwealth agency or state or territory authority;
- The practice believes it is reasonably necessary to lessen or prevent a serious threat to the life, health or safety of an individual or the public;

A government related identifier includes a Medicare number, Centrelink reference number, driver’s licence or passport number.

Example: the practice is not permitted to use Medicare numbers as the basis for patient identification. However, a practice can view and record Medicare numbers to verify the identification of a patient and for billing purposes.

APP 10 QUALITY OF PERSONAL INFORMATION

Practices must take reasonable steps to ensure the personal information it collects uses or discloses is accurate, up to date complete and relevant.

APP 11 SECURITY OF PERSONAL INFORMATION

Practices must take reasonable steps to protect the personal information it holds from misuse, interference, loss, unauthorised access, modification or disclosure.

Example: practices should issue staff with passwords to access patient databases that are changed on a regular basis, and store hard copy files in lockable filing cabinets or rooms, accessible only to authorised practice staff.

APP 12 ACCESS TO PERSONAL INFORMATION

The practice must, on request, provide a patient with access to their personal information within a reasonable time, unless an exception applies (see APP 6 above).

The practice is entitled to charge a 'reasonable' fee for access under the Privacy Act 1988 (Cth). The Victorian Health Records Act 2001 (Vic) sets specified fees for access to medical records. Further information on these fees can be obtained from AMA Victoria.

Any refusal must be accompanied by written reasons and information on how the patient may lodge a complaint.

APP 13 CORRECTION OF PERSONAL INFORMATION

A practice must take reasonable steps to ensure the personal information it holds is up to date, accurate, complete, relevant and not misleading. There is a positive obligation on practices to correct information where it is wrong.

The practice reasonably believes use or disclosure is necessary to take action in relation to suspected unlawful activity or misconduct of a serious nature

The practice reasonably believes use or disclosure is necessary for enforcement related activities of an enforcement body.

The practice must acknowledge a request for an amendment to their medical records, within a reasonable time. No charge can be made for the practice making the requested changes.

Example: Reception staff should confirm the contact details of the patient are up to date when they present for an appointment.

MY HEALTH RECORD:

The *My Health Record* system is the Australian government's digital health record system. It contains *My Health Records* which are online summaries of an individual's health information, such as medicines they are taking, any allergies they may have and treatments they have received. It was previously known as a Personally Controlled Electronic Health Record (PCEHR) or eHealth record.

A *My Health Record* allows an individual's doctors, hospitals and other healthcare providers (such as physiotherapists) to view the individual's health information, in accordance with their access controls. Individuals are also able to access their record online.

In most parts of Australia individuals need to actively register for a *My Health Record*. However, people whose registered Medicare address is in Northern Queensland or the Nepean Blue Mountains will have a *My Health Record* automatically created for them by the Australian Government unless they have opted- out by 27 May 2016.

The *My Health Records Act 2012*, *My Health Records Rule 2016* and *My Health Records Regulation 2012* create the legislative framework for the Australian Government's *My Health Record* system.

The My Health Records Act limits when and how health information included in a *My Health Record* can be collected, used and disclosed. The Office of the Australian Information Commissioner (OAIC) regulates the handling of personal information under the *My Health Record* system by individuals, Australian Government agencies,

private sector organisations and some state and territory agencies (in particular circumstances).
The OAIC's role includes investigating complaints about the mishandling of health information in an individual's *My Health Record*. The OAIC can also conduct 'Commissioner initiated investigations'.
The functions and enforcement powers available to the OAIC under the My Health Records Act and *Privacy Act 1988* include:

- investigating and conciliating complaints
- accepting enforceable undertakings
- making determinations
- seeking an injunction to prohibit or require particular conduct seeking a civil penalty from the Courts
- accepting mandatory data breach notifications from the System Operator, health care provider organisations, repository operators and portal operators

Collection, use or disclosure of *My Health Record* information is both a breach of the My Health Records Act and an interference with privacy.
Prior to a patient signing consent to the release of their health information, patients are made aware they can request a full copy of our privacy policy.