PRIVACY & DATA BREACH POLICY AND PROCEDURE

Purpose and Scope

This policy establishes the processes and procedure in place at Alma Street Medical (or "the Practice") to protect the privacy and confidentiality of all its patients and employees who are patients of the Practice. The Practice abides by all applicable federal and state laws when collecting, storing, accessing and transferring patient information.

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.

Legislation

Privacy Act 1988
Privacy Amendment (Private Sector) Act 2000
Privacy Amendment (Notifiable Data Breaches) Act 2017
Information Privacy Act 2009
Royal Australian College of General Practitioners - Standards

National Privacy Principles

The Privacy Amendment (Private Sector) Act 2000 extends the operation of the Privacy Act 1988 to cover the private health sector throughout Australia.

The Privacy Act requires our practice to abide by the 13 Australian Privacy Principles (APPs):

APP 1	Open and transparent management of personal information
APP 2	Anonymity and pseudonymity
APP 3	Collection of solicited personal information
APP 4	Dealing with unsolicited personal information
APP 5	Notification of the collection of personal information
APP 6	Use or disclosure of personal information
APP 7	Direct marketing
APP 8	Cross-border disclosure of personal information
APP 9	Adoption, use or disclosure of government related identifiers
APP 10	Quality of personal information
APP 11	Security of personal information
APP 12	Access to personal information
APP 13	Correction of personal information

For further information regarding complying with the legislation visit the website of the Office of the Australian Information Commissioner (www.oaic.gov.au).

Why and when your consent is necessary

When you register as a patient of our practice, you provide consent for our GPs and practice staff to access and use your personal information so they can provide you with the best possible healthcare. Only staff who need to see your personal information will have access to it. If we need to use your information for anything else, we will seek additional consent from you to do this.

We seek consent from our patients in the following circumstances when it falls outside of usual medical procedures or protocols:

- When we have student nurses, medical students or work experience students on site;
- When a third party will be present during your consultation for any reason;

- When any/all of your records are requested by a legal firm;
- When any/all of your records are requested by your employer;
- When any/all of your records are requested by another medical practice or allied health professional when there is no referral or transfer of records request in place;
- Any other situation where we require your consent to abide by the *Privacy Act 2009*.

Why do we collect, use, hold and share your personal information?

Our practice will need to collect your personal information to provide healthcare services to you. Our main purpose for collecting, using, holding and sharing your personal information is to manage your health. We also use it for directly related business activities, such as financial claims and payments, practice audits and accreditation, and business processes (e.g. induction and training of new staff).

What personal information do we collect?

The information we will collect 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 us 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 do we collect your personal information?

Our practice will collect your personal information:
- When you make your first appointment our practice staff will collect your personal and demographic information via your registration.
- When you provide feedback to us (in writing or electronically).

During the course of providing medical services, we may collect further personal information. This may be via Electronic Transfer of Prescriptions (eTP), MyHealth Record/PCEHR system or Medical Objects (e-Referrals).

We 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.

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 do we share your personal information with?

At times, we may be required to share your personal information:
- with third parties who work with our practice 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 (e.g. 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 (e.g. some diseases require mandatory notification);
- during the course of providing medical services, through Electronic Transfer of Prescriptions (eTP), MyHealth Record/PCEHR system (eg via Shared Health Summary, 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, our practice 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.

Our practice 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 do we store and protect your personal information?

Your personal information may be stored at our practice in various forms. We store all patient-related information electronically on our health information management system – Best Practice and Pracsoft (Medical Director).

Some software programs retain historical records on our server such as our WelchAllyn program (spirometry, ECG, etc). Any forms that you complete are scanned and imported to your personal health record and the hard copy is retained for a period of up to three (3) months in a secure cupboard. After three (3) months, we destroy hard copies in a secure manner.

Our practice stores all personal information securely.
Access to our computer system and server is highly secure. Each staff member and doctor is provided with a personal log in and password. In addition, each staff member and doctor signs a confidentiality agreement with the Practice upon commencement to abide by the privacy laws.

The system administrator (Practice Principal/Director) has the ability to lock patient records with a security code should any patient request that only their preferred doctor can access their health records.

Patients who become inactive on our system due to transferring to another medical practice or infrequent visits must have their records maintained for up to seven (7) years in accordance with patient health record keeping standards.

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

You have the right to access and correct your personal information. Our practice acknowledges patients may request access to their medical records. We require you to put this request in writing by completing a form at Reception (*Request to Access Medical Records*) and our practice will respond within a reasonable time. Allow for seven (7) business days to acknowledgement your request and a total of 14 business days to receive the request information by hand or registered mail. Please be aware there may be a cost associated with preparing and providing the records requested to you.

Our practice will takes reasonable steps to correct your personal information where the information is not accurate or up-to-date. From time-to-time, we will ask you 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. Please send your requests directly to our Practice Manager at practicemgr@almastreetmedical.com.

Notifiable Data Breaches

What is a Data Breach?
A data breach is when information that is private and confidential information regarding a patient is provided to, with intent or accidentally, to a third party without the consent of the patient.

The legislation now determines the severity and level of risk associated with a data breach to determine whether it is classed as a notifiable data breach.

This means having to report the breach to the patient, any third parties who received the information and should not have, and/or to the (Australian Office of Information Commissioner (AOIC).

How do Data Breaches occur?
Data breaches occur in a number of ways. Some examples include:

- lost or stolen laptops, removable storage devices, or paper records containing personal information
- hard disk drives and other digital storage media (integrated in other devices, for example, multifunction printers, or otherwise) being disposed of or returned to equipment lessors without the contents first being erased
- databases containing personal information being ‘hacked’ into or otherwise illegally accessed by individuals outside of the agency or organisation
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment
- paper records stolen from insecure recycling or garbage bins
- an agency or organisation mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address, and
- an individual deceiving an agency or organisation into improperly releasing the personal information of another person.

How is a data breach assessed?
To determine what other steps are immediately necessary, agencies and organisations should assess the risks associate d with the breach. Consider the following factors in assessing the risks:

- The type of personal information involved.
- The context of the affected information and the breach.
- The cause and extent of the breach.
- The risk of serious harm to the affected individuals.
- The risk of other harms.

Once the assessment has been made, the Practice will follow the appropriate steps to record and report the breach appropriately and as required by the legislation.

What is a Notifiable Data Breach?
A notifiable data breach is an incident that has been assessed as meeting all of the above criteria. This breach needs to be reported to all persons involved (the patient, any third parties) and the Commissioner.

What are your obligations and who do you report it to?
If you have accidentally breached privacy, or have become aware of a breach in privacy, report it immediately to the Practice Manager so that it can be recorded, assessed and appropriate action taken.

Risk management and prevention
There are four (4) key steps to consider when responding to a breach or suspected breach:

Step 1: Contain the breach and do a preliminary assessment
Step 2: Evaluate the risks associated with the breach
Step 3: Notification

Step 4: Prevent future breaches

Data Breach Register
We have developed a data breach register to start recording all breaches, regardless of classification, to ensure that we follow best practice regarding the protection of information housed on our systems and the privacy and confidentiality of all of our patients.

Please remember to report any breaches to the Practice Manager to make an assessment and action accordingly.

Response Team

The following roles will be held responsible for responding to any data breach notifications/claims made against the practice:

- Practice Principal
- Practice Manager
- Practice Administrator

With assistance as needed from **Shawn Munster (Rescue Biz Systems)** for any system and security breaches to the practice server.

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. Please send your concerns to our Practice Manager via email – practicemgr@almastreetmedical.com.

Our Practice Manager will acknowledge receipt of your complaint and attempt to resolve your concerns as soon as possible. Due to the nature of our industry and depending on the nature of your complain, please allow for up to 14 working days on a final outcome.

If you're not satisfied with the response we provide to you, you may also contact the OAIC. Generally the OAIC will require you to give them time to respond, before they will investigate. For further information visit www.oaic.gov.au or call the OAIC on 1300 336 002.

Privacy and our website (including social media pages)

When you submit a form or choose to contact us via our website or social media pages, please be aware that the digital information we receive may be collected and used for the following reasons:

- To contact you as per the details you have provided;
- To update your personal health record at your request;
- To follow up on any feedback or complaints that you have submitted via our website or social media pages;
- To respond to a general enquiry that you have submitted via our website or social media pages.

Please be aware that as with any website or social media page, the personal details you submit may be used in website analytics, cookies, etc.

Every employee of this practice is aware of the privacy policy and has signed a privacy statement as part of their terms and conditions of employment. This privacy statement continues to be binding on employees even after their employment has terminated.

Policy review statement

This privacy policy will be reviewed annually or as required to ensure it is in accordance with any changes to legislation that may occur. A copy of this policy will be accessible on our website as well as within the Practice. Our Practice Manager will retain hard copies of all policies and procedures which can be accessible upon request.

Document Control

Version	Date Created/Modified	Reason for Change	Review Date	Personal Responsible
1.0	01/10/2015	-	Oct 2016	Shantal Wallace
1.1	30/05/2016	Update position Practice Manager	May 2017	Shantal Wallace
1.2	05/07/2017	Update company logo, review content & add Document Control	Jun 2018	Shantal Wallace
2.0	23/02/2018	Incorporate Data Breach Procedure	Feb 2019	Shantal Wallace
2.1	Mar 2019	Update IT contractor and contact details	Mar 2020	