practice building solutions

outstanding performance+

Privacy Policy

Virtual Medical Office Pty Ltd

Trading as VMORE Health

ABN 20 129 664 240

rouselawyers.com.au

Unit 4, 92 Commercial Road
Newstead Qld 4006

Locked Bag 22
Fortitude Valley BC Qld 4006

T 07 3648 9900
F 07 3648 9911
E admin@rouselawyers.com.au

Privacy Policy

Effective From March 2014

1. Introduction

This Policy outlines how we deal with "personal information", which is information about an individual whose identity is apparent, or can reasonably be ascertained, from that information (**Personal Information**).

Virtual Medical Office Pty Ltd (ACN 129 664 240) (we, us or our) has adopted this Privacy Policy, in accordance with the Australian Privacy Principles in the Privacy Act 1988 (Cth) (**APPs**).

We collect Personal Information, including health information, in the course of operating a private specialist medical practice management system through hosted software (**Services**). Our clients are health professionals and associated organisations using our Services to manage their practices (**Clients**).

Our staff access the Services to facilitate configuration, database maintenance, management reporting, patient appointments, billing of professional services, transcription of clinical correspondence and supporting our clients in the day-to-day operations of their practice.

We welcome your comments on this policy or any of our information management practices, including de-identification practices. Please see below for contact details.

2. How we collect Personal Information

We collect Personal Information in four main ways:

(a) collecting specific information relevant to providing our Services to Clients (**Active Collection**);

(b) automatic electronic collection online, in accordance with standard business practice on the Internet (**Automated Collection**);

(c) generalised passive collection when Clients use our Services to collect and store personal information about their patients, customers or themselves (**Passive Collection**); and

(d) collecting Personal Information from persons other than the individual to which it relates (**Third Party Collection**).

We engage in Active Collection when an individual or organisation:

(a) (**Registrations)** registers or subscribes for a service, list, account, membership, connection or other process whereby that individual enters his or her details to apply for, receive or access something, including a transaction;

(b) (**Services**) access or uses the Services; or

(c) (**Contact**) contacts us via any medium, including telephone, fax or email.

We engage in Passive Collection whenever Clients include any personal information about their patients or themselves in any content they record or store through our Services. For example, this occurs when:

(a) (**Client documents and databases**) Clients use our Services to record, store or communicate data about their patients, including notes, correspondence, documents, records, calendars or databases containing personal information; and

(b) (**Incidental Client information**) Clients use our Services to record, store or communicate notes or files about their patients which also contain information about themselves, such as their business name, letterhead, address, phone number, or location.

We and some of the third party services providers we use (such as Google Analytics) engage in Automated Collection as follows:

(a) (**Logs**) when you visit our website or use the Services, our server and analytics service may log details about your visit such as your IP address, the time and duration of visit, the link from which you visited, and information about your browser and operating system; and

(b) (**Cookies**) we will likely place a cookie on your device when you visit our website.

We engage in Third Party Collection when a third party refers us business.

3. The kinds of Personal Information that we collect and hold

Through the processes above, we will collect the following categories of Personal Information about individuals:

(a) (**Sensitive Health Information**) information or opinions recorded on our Services by our Clients about individuals' health, health services, or wishes regarding health care and information collected by our Clients and stored on our Services to provide, or in providing, a health service of any kind, including:

(i) medical records;

(ii) genetic information;

(iii) health tests and test results;

(iv) medical correspondence;

(v) medical appointments and referrals; and

(vi) medicines taken or prescribed.

(b) (**Identity Information**) name, signature, location, website address, date of birth, nationality, license & registration details, bank account details, family details, employment details, educational qualifications and third-party usernames, Medicare and health fund details;

(c) (**Contact Information**) email address, social media profiles, telephone & fax number, third-party usernames, residential, business and postal addresses;

(d) (**Behaviour Information**) associations, memberships, finances, purchases;

(e) (**Internet Data**) operating system, domain name; and

(f) (**Business Information**) information about a business or project, if it is run in the individual's personal capacity, including information on professional affiliations or services offered.

4. How we hold Personal Information

We hold and store Personal Information using:

(a) (**Storage and Hosting Services**) third party data services, which are businesses that professionally manage information technology infrastructure;

(b) (**Software Services**) third party application providers, where we use an application for the purposes of our business and store data in association with that application on infrastructure provided by those third party application providers;

(c) (**Business Devices**) devices operated by employees of our business; and

(d) (**Paper Files**) printed paper and our own secure archival storage.

We may combine or link Personal Information about you that we collect on one occasion with Personal Information about you that we collect on other occasions.

All sensitive documents no longer required are placed in a locked document destruction bin. We receive confirmation of destruction for each scheduled removal.

5. How we secure Personal Information

We and our employees, contractors and other authorised representatives will take reasonable precautions to protect Personal Information from unauthorised access. This includes appropriately securing our physical facilities and electronic networks.

We secure Personal Information that we collect by:

(a) (**Credentials**) using authentication credentials for each portion of the data storage infrastructure that we control in accordance with best practice;

(b) (**Encryption**) using specialized encryption algorithms and software to protect passwords and forcing one-way encryption to prevent reverse-engineering of these the passwords that we generate;

(c) (**Session Expiry**) forcing time-out of authentication sessions and requiring re-authentication to minimise risk associated with idle connections;

(d) (**Firewalls**) using both server and network firewalls to control access points in and out of the data storage infrastructure;

(e) (**Network Traffic Encryption**) using Secure Sockets Layer (SSL) technology to secure transmissions both to and from the data storage infrastructure; and

(f) (**Reputable Vendors**) ensuring that the third party providers holding data and information on our behalf are reputable vendors taking reasonable steps to secure the information.

By using any part of the Services, individuals acknowledge that the security of online transactions and the security of communications sent by electronic means or by post cannot be guaranteed. Individuals provide information, including Personal Information, to us via the Services at their own risk. We cannot accept responsibility for misuse or loss of, or unauthorised access to, Personal Information where the security of information is not within our control.

6. The purposes of collection, holding and use

We collect, hold and use Personal Information for the purpose of providing the Services, improving them and developing additional functionalities for our users.

For **Passively Collected Personal Information,** the collection, holding and use of information happens simply by virtue of Clients using the Services. It is part of the Service to allow Clients to manage the provision of health services by entering, storing, organising and accessing data about patients through the Services.

We access Client software and the Personal Information stored and processed on it to facilitate:

(a) software configuration;

(b) database maintenance;

(c) management reporting;

(d) patient appointments;

(e) billing of professional services;

(f) transcription of clinical correspondence; and

(g) generalized support to our Clients in the day to day operations of their practice.

For **Actively Collected, Automatically Collected and Third Party Collected Personal Information,** our handling of Personal Information includes holding and using the Personal Information so that we can:

(a) (**Identify**) identify Clients for the purpose of providing the Services;

(b) (**Communicate**) communicate with Clients for the purpose of providing the Services, including notifications, support; communications about our goods and services; marketing and promotions; and competitions, surveys and questionnaires;

(c) (**Transact**) transact with clients for the purpose of providing the Services; and

(d) (**Business Development and UX**) assess the progress and success of our Services, develop business opportunities, enhance clients' experience of our Services; and

(e) (**Secure access**) providing secured access to Clients using an account and allowing users to retrieve their password if they forget it.

The purpose of automated collection online is not to identify specific individuals. Rather, it is generally used for data analysis. For example, we may use cookies and log information to ascertain the number of unique visitors to our website, whether or not those visitors are repeat visitors, and the source of the visits.

7. How and when we share or disclose Personal Information

Our Service permits and facilitates our Clients communication of health information to other health service providers and professionals for the purposes of providing health services. Recipients of such information include:

(a) specialist practitioners;

(b) alternative health service providers;

(c) diagnostic testing facilities; and

(d) general practitioners.

Our Services allow internal communications between our Clients. We also use Medical Objects and Healthlink for secure electronic messaging. These organisations' privacy policies are available at:

(a) www.medical-objects.com.au/privacy; and

(b) http://www.healthlink.net/en_US/about-us/privacy-policy/

In some cases, it will also be necessary for us or our clients to disclose health information to a person responsible for a patient such as a parent, guardian, power of attorney, spouse, partner, or relative. This will be the case, for example when the disclosure is:

(a) necessary to provide appropriate care or treatment of the individual; or

(b) made for compassionate reasons.

When we use third party service providers to help us provide and maintain our Services, this may involve providing them with some degree of access to Personal Information. These third party service providers include:

(a) (**Hosting**) Cloud and web hosting service providers;

(b) (**Saas**) providers of software as a service;

(c) (**Support**) providers of IT support services, web and software development; and

(d) (**Online payment**) providers of online payment systems;

We will only share Personal Information with these third parties to the extent reasonably necessary to perform their functions, in order to make our Services more effective and affordable.

By using any part of the Services, individuals acknowledge that we are not responsible for the privacy or security practices of any third party (including third parties that we are permitted to disclose or transfer Personal Information to in accordance with this Privacy Policy or any applicable laws). The collection and use of Personal Information by such third parties may be subject to separate privacy and security policies. For more information on the third party service providers we use, and their privacy policies, please contact us using the details listed below.

For information on disclosures to overseas recipients, see below.

8. Contacting us to access, change or delete Personal Information

Clients may edit content and account details within the Services.

Individuals concerned about their Personal Information can also contact us using the details below to:

(a) request access to the Personal Information that we hold about them; and

(b) correct Personal Information that we hold about them; or

(c) ask us to delete their accounts permanently including content on it.

Position Title:	Managing Director
Telephone:	1300 725 145
Email:	privacy@vmo.net.au
Postal Address:	PO Box 52, Everton Park, Queensland 4053

We reserve the right to refuse access or correction where there are reasonable grounds for doing so, for example if:

(a) the request is frivolous;

(b) providing access would be unlawful or would compromise the privacy of another person; or

(c) the requested correction would result in information being misleading or inaccurate.

9. Complaints

(a) If you have a complaint relating to an alleged breach of the APPs, you should contact us using the details listed in the previous section of this Privacy Policy.

(b) When you notify us of a complaint about our handling of your Personal Information, we will deal with the complaint by responding to it in writing within a reasonable period (usually 10 business days from the day we receive your email).

(c) We will endeavour to work with you to resolve the complaint entirely within 30 days, although that period may be longer if it is reasonable to take longer given the nature of your complaint.

(d) If you are unsatisfied with our response, you may make refer the complaint to the Office of the Australian Information Commissioner (http://www.oaic.gov.au/) or to the NSW Privacy Commissioner, the Queensland Information Commissioner or Victorian Health Services Commissioner, if your complaint relates to our handling of your health records in that state.

10. Disclosure of Personal Information to overseas recipients

(a) Our use of third party service providers is usually within Australia, but may nonetheless result in the processing of your Personal Information overseas. You may not have the same rights in relation to the handling of your Personal Information by overseas recipients as you would under Australian privacy law.

(b) By providing us with Personal Information, you consent to the transfer of your Personal Information to recipients outside Australia.

(c) If you consent to such transfer, we will not be accountable for overseas recipients' handling of your Personal Information. In any event, we take reasonable steps to ensure that the Personal Information that has been transferred will not be held, used or disclosed by the recipient of the information inconsistently with the APPs.

11. Amendment

We may amend the Privacy Policy at our sole discretion. If you continue to use the Services after receiving notice from us of such an amendment to the Privacy Policy, you agree to be bound by the Privacy Policy as amended.