Magentus

Privacy Policy

Magentus Practice Management Pty Ltd ACN 086 370 130 (**us, we, our**) is subject to the *Privacy Act 1988* (Cth) (**Act**), the Australian Privacy Principles (**APPs**) and we may also be subject to other privacy and health data protection laws applicable in Australia (together, **Privacy Laws**). Your privacy is important to us and we are committed to ensuring that your personal information is handled and protected in accordance with all relevant Privacy Laws.

This Privacy Policy (**Policy**) sets out how we may collect, access, hold, use and disclose (together "**process**") personal information in the course of providing our products and services (and operating our business).

By accessing our website (www.magentus.com/practice-management) (**Site**) or using our products and/or services, you consent to the processing of your personal information in accordance with this Policy.

This Policy also applies to personal information that we receive from our customers when they use our software products or receive other services from us. Our customers are primarily health service providers that use our software to store and manage patient information and records – so this Policy also applies to any patient data that is stored in our software by those customers (or their staff) and that we process on their behalf (**Patient Data**).

If you have any questions or require any further information about this Policy or our privacy practices, you can contact our Privacy Officer. Their contact details are available at the end of this Policy.

What is personal information and sensitive information?

"Personal information" is any information (or an opinion) about an identified individual or an individual that is reasonably identifiable.

"Sensitive information" is a category of personal information and specifically refers to information or an opinion about more sensitive things like an individual's racial or ethnic origin, religious beliefs or affiliations, sexual orientation or practices, criminal record, and health information.

Collection of personal information

What personal information do we collect directly?

The personal information that we may directly collect while providing our products and services (and marketing those products and services) includes the following (in each case, relating to our customers, potential customers, contractors, suppliers and their staff):

- contact information, such as name, position, practice, office and postal address, email address and phone, facsimile and mobile telephone numbers;
- subscriber name and/or practice name;

- position or title (such as doctor, specialist, practice manager, receptionist, IT consultant or otherwise);
- practice type (such as general practitioner, dermatologist, general surgeon, orthopaedic surgeon or otherwise);
- information about devices (and number) requiring access to our software products;
- usernames and email addresses;
- billing information, such as bank account details; and
- any other additional information provided to us by those entities and individuals.

What personal information do we collect via our customers?

As noted above, we provide software products and services to assist health service providers to manage their practices, including by enabling them to store and manage Patient Data. Under the terms of the Master Service Agreement that we enter into with each of our customers, we may have access to their Patient Data to process it on their behalf. Patient Data is likely to include sensitive information, including information about a patient's:

- health conditions or disabilities;
- use or receipt of particular health services or treatments (or their request to receive particular health services or treatments);
- dietary requirements;
- medical history and test results;
- general practitioner and other specialist practitioners that have treated or advised them; and
- Medicare and health insurance details (including their claims history),

and other information collected by the relevant health service provider and stored within our software.

How do we collect personal information?

The table below lists the main ways that we will collect personal information:

How we collect personal information	Examples of when this may occur
Directly from you	– When you contact us (e.g. by phone, email or online enquiry). – When you create an account to use our software or sign-in to use our software. – When you contact us seeking technical support in relation to our software or integrations with other services. – When you subscribe to receive news and other marketing updates from us. – When you attend seminars and functions run by us.

	– When we engage you or your employer as a contractor or service provider or we otherwise interact with you in the course of our general business activities.
From third parties	– When you are an employee or contractor of a health service provider and that health service provider creates an account for you to use our software or nominates you as a contact person in relation to the health service provider's account with us. – When you are a patient of a health service provider that uses our software, and your personal information is entered into the software by that health service provider (or by their staff) or through integrations with other digital systems used by that health service provider (e.g. My HealthRecord etc). – When a medical practitioner requests information (e.g. healthcare images or results such as X-Rays or pathology test results) from a third party through our software.
From or through automated services	– When our website stores a cookie in your browser. – When our web-analytics services log your IP address.

When we receive Patient Data from our customers or third-party services used by our customers, we are the processor, and our customers are the controllers, in relation to any personal information subsisting in that Patient Data. When we process personal information (including Patient Data) on behalf of our customers, we do so in accordance with their instructions. Please refer to the privacy policy of the relevant health service provider with whom you have dealings for more information on how they handle your personal information – we are not responsible for (and cannot control) how those organisations handle your personal information.

All personal information that we collect is reasonably necessary for the purposes directly relating to providing our products and services to our customers and conducting our general business activities.

In the circumstances where you voluntarily provide us with personal information, we will take this as your implied consent for us to collect your personal information. However, we will construe this implied consent narrowly and will not rely on it to handle your personal information in a manner that is not directly related to the purpose for which your personal information was

provided or for a purpose outside your reasonable expectations.

Consequences if personal information is not collected

If we are unable to collect the personal information that we reasonably require, then we may not be able to provide our services to you (or otherwise interact with you while carrying out our business activities).

Cookies

"Cookies" are small data files that may be downloaded to your computer when you visit a website, which may be used to track your use of that website. Cookies must be enabled in order to use web based software products offered by us and may be used to provide users of your computer with information that we think may interest the users of your computer.

We may use cookies from time to time to:

- track your usage of our software products;
- improve your experience within our software products;
- provide you with better service when you use our software products;
- authenticate your access to our software products; and
- recognise you when you return to our software products.

This information may be linked to any personal information you may provide and may be used to identify you. You can adjust your internet browser to disable or warn you when cookies are used. However, disabling cookies will stop our software products from functioning fully.

Use and disclosure of personal information

Personal information that we have collected directly

In relation to personal information that we have collected about you (and which is not Patient Data), we process that personal information for the following purposes:

- to provide and deliver our products or services to you and our customers;
- to communicate with you and administer our relationship with you;
- to discuss potential updates or advances to our products with you, and to keep you informed of relevant upcoming events and activities;
- to address any query, feedback or complaints you may have, and to record your marketing and communication preferences;
- to manage our business;
- for marketing and research purposes related to us or our partners (subject to any applicable laws including the *Spam Act 2003* (Cth) and *Do Not Call Register Act 2006* (Cth));
- to fulfil and comply with any legal, enforcement (including debt recovery), regulatory and contractual obligations (including any requirements under our Master Service Agreement); and

- to fulfil any other purpose that was made clear at the time of collecting that personal information.

If we hold personal information about you that was collected for a particular purpose, then we will not use or disclose that information for another secondary purpose without your consent, unless:

- you would reasonably expect us to use or disclose the information for that secondary purpose; or
- that use or disclosure is required by law; or
- the use or disclosure is otherwise permitted under Privacy Laws.

Patient Data

In relation to Patient Data, we only process that personal information for the following purposes:

- to provide and deliver our products and services to our customers;
- to de-identify that Patient Data so that it no longer contains any personal information.

When we process Patient Data, we only do so in accordance with the instructions of our customers or to the extent required for our customers to use the features of our software that they have subscribed to use.

Disclosure to third parties

We will not disclose your personal information to any third party other than as set out in this Policy (or as required by law, to protect our rights or property, or to avoid injury to any person). In order to deliver the services that we provide to our customers (and for our software to properly function), we may need to disclose personal information (including Patient Data) to other organisations. Any such disclosure is limited to the extent reasonably required to provide those services.

Key examples of third parties that may receive personal information from us are:

- our customers (and their staff) that access personal information about you when using our software;
- cloud service providers used to host and deliver our software (refer to the "Storage and Security" section below);
- other technology services with which we have partnered (or that our software integrates with) in order to deliver our services, such as:
    - patient apps;
    - online Australian government apps;
    - online appointment booking and reminder services;
    - remote patient monitoring services;
    - SMS and other electronic messaging services;
    - integrations with medical devices;
    - payment systems (e.g. HICAPS and EFT); and
    - other third-party integrations subscribed to by our customers.

We take reasonable steps to ensure that any third-party organisations that may receive personal information from us are bound by privacy and data security obligations in relation to the storage and protection of that personal information.

Our customers may also use our software to share and disclose Patient Data (such as when they are referring their patients to other specialist health service providers or ordering tests on behalf of their patients). This type of disclosure by a health service provider is controlled by that health service provider and is governed by the privacy policy of the relevant health service provider.

Overseas

We do not transfer or store any of your personal information to people overseas, however third parties that we may partner with or whose products or services we may use or integrate (**Partners**), may do so. Countries to which our Partners may transfer your personal information include but are not limited to the United States of America, the United Kingdom and countries in the European Union.

Personal information that is stored overseas may not be subject to the Privacy Laws. By providing your personal information or using our services, you consent to this transfer.

Although we do not have a presence in, or target our services towards customers in the European Economic Area (**EEA**) or the United Kingdon (**UK**), if you access our services from the EEA or the UK, you may have additional rights under the General Data Protection Regulation (**GDPR**) in respect of any of your personal data that we obtain.

If you believe the GDPR may apply to your personal data and you wish to exercise any of your data subject rights, please send your request in writing to our Privacy Officer (using the contact details available at the end of this Policy).

External links

Our Site and the software products offered by us may from time to time contain links to other websites, and those third-party web sites may collect information about you. You acknowledge that linked sites are not operated by us, and we take no responsibility for the content or privacy practices of the operators of other websites that are linked to our software products or Site.

Marketing

You acknowledge and agree that by using our products or services we may, from time to time, use personal information collected by us for our marketing and research purposes. This may include sending updates and information related to us or our activities by post, telephone or any form of electronic communication. We may also share your personal information with our Partners who may use any email address or other contact information you provide to us at any time for the purpose of contacting you about their products or services, or other offers or promotions.

By using our products or services, you are "opting-in" to us (or any Partners to whom we may provide your personal information in accordance with this Policy), sending you communications

as noted in the previous paragraph. You can, at any time, opt out of receiving our marketing material by contacting us (or in the case of marketing material of a Partner, by contacting that Partner). Once you opt out of receiving marketing material from us, you acknowledge and agree that this removal from our distribution lists may take several business days after the date of your request to be removed. You acknowledge and agree that even if you opt out of receiving marketing material, we will still send you essential information that is necessary, or we are legally required, to send you relating to the services we provide.

We do not use Patient Data for marketing purposes (or share Patient Data with third parties for marketing purposes). We only use Patient Data for the purpose of delivering our products and services in accordance with this Policy and our Master Service Agreement with the relevant customer.

Research and Data Analytics

We may, from time to time, conduct data analytics on data relating to the use of our software products and services. We may use data generated from data analytics processes for the purpose of interpreting the usage of our software products, to evaluate, improve and develop our software products, or for our internal business purposes.

Storage and Security

We take reasonable steps to protect personal information from misuse, interference and loss, unauthorised access, modification or disclosure and to comply with the APPs and any other applicable Privacy Laws. This includes adhering to good industry practice in relation to data security and the prevention of data loss. Our information security management systems are ISO 27001 certified (which is a voluntary international standard on information security).

To the extent that we hold personal information digitally, it is stored in Australia, and we take reasonable steps to ensure it is held securely and stored on infrastructure that is either owned or controlled by us or a reputable third-party service provider (for example, a cloud storage provider) and is encrypted. Temporary access is only provided to those of our employees who require access to the records in the course of their duties in providing our customers with our products or services, such as troubleshooting and checking system functionality. Where we use a third-party service provider, we take reasonable steps to ensure that they comply with the Act and any other applicable Privacy Laws.

Notwithstanding the reasonable steps taken to keep information secure, security cannot be guaranteed and data breaches may occur. In the event of a security incident, we have in place procedures to promptly investigate the incident and determine if there has been a data breach involving personal information, and if so, to assess if it is a breach that would require notification under applicable Privacy Laws. If it is, we will notify affected parties in accordance with the Act (or where we do not have a direct relationship with the affected individuals, we will cooperate with the party who has the closest relationship with the affected individuals to notify them).

If you reasonably believe that there has been unauthorised use or disclosure of your personal information, please contact us immediately.

Destruction and De-Identification of Personal Information

Where we hold personal information, and the information is no longer needed (or no longer required by law to be retained by us), we will take such reasonable steps in the circumstances to destroy that personal information or to ensure that the information is de-identified.

Any files that are destroyed are done through secure electronic destruction processes.

Changes to this Policy

We may make changes to this Policy from time to time to take account of changes to relevant laws and technology, changes to our business operations and practices and general changes to the external business environment. A current copy of the Policy is maintained on our Site. All personal information held by us will be handled in accordance with the most up-to-date version of the Policy. If you use our products or services after a change is made to the Policy, we will take that as your consent to the updated Policy.

Contact Us

Access and accuracy of personal information

You have the right under the Act to seek access to or correct your personal information held by us if it is inaccurate, incomplete, out of date or misleading. If you want to access your personal information, or if you believe that it is inaccurate, incomplete, out of date or misleading, please contact us in writing (see below).

We will respond to any such request within a reasonable period and we will grant access provided the request does not fall under one of the exceptions to access stated in the APPs. We may charge a reasonable fee for providing that information.

Access may be denied in certain circumstances permitted under the Act (such as where the request creates a serious threat to the life or safety or is otherwise unlawful).

If you are an individual seeking to access and correct your Patient Data, you should initially contact your health service provider or health service practice.

Enquiries and complaints

If you want to make a complaint about our management of personal information, to correct information or to request further information, please contact us. Our Privacy Officer will contact you about your complaint or request as soon as reasonably practicable and we will attempt to resolve it with you.

If you are not satisfied with the outcome of your complaint or request, you may refer the matter to the Office of the Australian Information Commissioner by visiting the website www.oaic.gov.au. Further information about the Act and the APPs is also available from the Office of the Australian Information Commissioner.

Contact details

If you wish to contact us in relation to any privacy related matter, please use any of the following methods of contact:

Email: pmprivacy@magentus.com
Phone: 1300 889 362
Address: PO Box 2034, Fortitude Valley QLD 4006

Last update: November 2023