



info@mediclinic.com.au

<https://mediclinic.com.au>

TEL: 61 3 9947 1981

info@mediclinicsoftware.de

<https://mediclinicsoftware.de>

TEL: 49 6925 7377 482

PRIVACY AND SECURITY AND ACCEPTABLE USE POLICIES AND PROCEDURES FOR USE OF MEDICLINIC SOFTWARE – in addition to our standard terms and conditions on our website.

Mediclinic Software comprises the following companies but may change from time to time according to new growth and expansion. These **Security and Policy and Terms and Conditions** of use comprise the agreement for using or software based on a software as a service model. (SAAS). We ask that you read and accept these terms before you commence use of our software. These may be downloaded at any time from our website

<https://portal.mediclinic.com.au/Account/LoginV2.aspx>

The companies operating various parts of the whole of services we supply to you the customer are as follows:

BANCER PROPERTY PTY.LTD. ATF BANCER PROPERTY FAMILY TRUST T/AS MEDICLINIC SOFTWARE

Bancer Property Pty Ltd trading as Mediclinic Software

Mediclinic Software Pty Ltd

Mediclinic software (Thailand) Company Limited

Mediclinic Asia Pacific Corp

Mediclinic Software Europe KFT

Mediclinic Software Germany GMBH

Mediclinic Software has Head Office Operations in **Berlin Germany and Melbourne Australia** where patient data storages, privacy security and laws on Spam and other matters are reciprocal under various Government laws in place including Australian Privacy Acts and legislation. We also have offices in Budapest Hungary as well as offices in Philippines – support only functions and United Kingdom (London) and United States – support functions only. We also have Programming functions and in Chiang Mai Thailand. Our head Office functions are in countries with the HIGHEST WORLD Business and Data standards.

As a part of providing services to you, we may use third party suppliers and contractors and we may use staff located in other countries. If we elect to do this, it is because it is an essential part of us being able to fully provide services to you that meet the strict requirements of a cloud SAAS service provider. As an example of 3rd parties we may use, we may use Financial services providers to enable Credit Card billings, security checking and testing and the Servers we use are owned and operated by Microsoft and their partners. This is not the full list of 3rd party suppliers. Some of our 3rd party suppliers remain confidential and we may not be able to disclose who they are due to Governance requirements imposed upon us by governments. If we can disclose suppliers, we will upon request.

CONFLICT OF INTEREST

Mediclinic Software **does not operate own or have any financial or other interest** in any other business apart from providing software as a Service to you. Should any of your staff or any of our staff try to work together in any manner that is not part of the operations which they were first engaged in, that is to say, if they try to set up any business venture that they



info@mediclinic.com.au

<https://mediclinic.com.au>

TEL: 61 3 9947 1981

info@mediclinicsoftware.de

<https://mediclinicsoftware.de>

TEL: 49 6925 7377 482

may wish to access privileged information, we will block all access and dismiss our staff and advise your Managers accordingly. We also ask that you do not try to engage any of our staff services outside of the scope of support services to you.

Mediclinic Staff are strictly prohibited in their employment agreements from working with any client or service provider of Mediclinic Software for a period of 5 years after their termination with any of our companies.

All Mediclinic Staff are prohibited from performing any work whether paid or unpaid for any client or customer outside the scope of support duties in the performance of their work for Mediclinic Software or support to our clients and customers.

ACCEPTABLE USE BY CLIENT AND MEDICLINIC SOFTWARE STAFF & SUPPLIERS

How do we identify who we are to receive instructions from?

Mediclinic Software works similar to banks where we must KNOW YOUR CUSTOMER. In this regard we speak to someone at your organisation. We get something in writing from you and we get a credit card or other form of identity or authorisation. If you are a Medical Provider, we have access to records that can identify you to ensure your legality and rights to use our software. If you are not a Medical Provider, we may get a formal agreement between us.

Our software may be used for many purposes not just health. We can also provide a client database so you can provide services to your customers such as online bookings customer management and other services. We will do whatever is required to verify your identity and ensure no spam or untoward actions are placed for use of our software.

Mediclinic Software may provide you with access to services which enable payments from other parties such as Government and Banks or other financial companies. As part of this we expect that you will **at all times** ensure your staff and users within your Client Database adhere to applicable legal, statutory, or regulatory compliance requirements terms and conditions by us and Government rules, regulations and expectations at all times.

Mediclinic Software does not monitor every use of your database for legal compliance as this is up to you. **HOWEVER**, if we are notified by relevant legal authorities that you or any user, is performing a breach of your legal requirements, we may without notice suspend you or any user from access to the servers we operate. If permitted, we may contact the appropriate person within your organisation on how to proceed further.

Mediclinic Software ensures that we employ staff who are vetted for security in compliance with requirements set down by the governments where that person is employed for us or by us.

PRIVACY POLICY AND HOW WE MANAGE YOUR DATA

To keep our Privacy Policy SIMPLIFIED, we do not use any data or information for any purpose whatsoever other than in the performance and duty of providing a service to you or your clients or patients in a legal and secure manner.



info@mediclinic.com.au

<https://mediclinic.com.au>

TEL: 61 3 9947 1981

info@mediclinicsoftware.de

<https://mediclinicsoftware.de>

TEL: 49 6925 7377 482

No data is on-sold or used for marketing in any way. WE RESPECT SECURITY AND PRIVACY at all times.

In Australia, we are under Australian Government rules and laws and we abide by those rules always. We only store and manage data under these rules and in accordance with the Privacy Principles under law. In Europe, UK, USA and any country where we operate we also comply with or exceed the laws of those respective countries. We are not interested in selling or using your data you place with us in trust and we respect that and we do everything we can to ensure that data is always protected often exceeding requirements set by Government or other bodies.

At all times, we never share this data or information with any company, body or person unless it is required by law, or instructed under a court or Government directive. The data we hold is only used in a way so that you the user of our software may manage your business for the benefit of your patients or clients. We do not interfere in this process.

We are a Software as a Service model and we have no interest in your data other than providing a service so you may perform your business duties in a legal manner.

By agreeing to the use of our software it is also your responsibility to ensure the security of passwords, usernames and log in at all times of all your users and staff and people you authorize to use the software we provide.

You also agree that in allowing us to maintain this data for you that at times we may use our associated services to perform these functions for you both within and out of the country in which you operate our software but at all times complying with the Australian Laws or the laws of the country in which we provide the software services to you.

OVERSEAS ACCESS

You Agree by use of our software and the signing in and use of our software and your database, that at times DATA MAY BE ACCESSED OVERSEAS by Mediclinic Software staff, suppliers and 3rd parties. We may use 3rd party developers, security advisers and others for certain functions.

For the purposes of software development data deployments, security checking, services provision, and various other methods required to operate a Successful Multi national business with partners who are overseas based supplying services to us and our clients your data may be accessed or sent overseas for the purpose of providing a service to you. The overseas access is only for the time of the required use of that piece of data and not all data. For example we may have one of our staff assisting you with a patient or client issue so our staff which may be in another country will access this piece of data to assist you. You may also need help from a bank located overseas for the processing of a payment and this piece of data is sent to them for processing to assist you. Data is not stored or distributed permanently outside of the realm in which the client is legally operating. We also employ services from various Microsoft partners in the supply of our Cloud environment and they may at times need to be located overseas when providing services to us to assist you.



info@mediclinic.com.au

<https://mediclinic.com.au> TEL: 61 3 9947 1981

info@mediclinicsoftware.de

<https://mediclinicsoftware.de> TEL: 49 6925 7377 482

USE AND COMPLIANCE BY USER

Mediclinic Software provides a separate database for each of our clients. Within this database you may store images, files, documents and data. We do not restrict what you can store or how much data you store.

Each user is provided with a username & passwords that are unique to that database.

The user is to then set for themselves, 2 passwords, 1 set being 8 blocks and the 2nd of 12 blocks. It is compulsory for the 2nd set to contain numbers, upper and lowercase letters and symbols; and the option of 2 factor Authorisation which we STRONGLY RECOMMEND.

Within your database, Mediclinic Software provides a system where you the user controls who has access to and what access a user within your organisation has at all times. You control new users, the deletion of users and rights. We have various STAFF roles that allow you to set these as well as a menu option chart of rules you can add or take away user rights and access. You may at any time reactivate any user account you have deleted.

Mediclinic Software does not monitor your staff or delete or add users for you. This remains your responsibility. We may at time have need if instructed by legal authorities to act in a way to prevent you or staff accessing data. We will act only if requested by your site administrator.

Mediclinic Software provides various layers of security and user access. We control the first layer – your administrator and privileges. You may at any time create or delete any user account for your own purpose. At all times you the client has control for roles and responsibilities for provisioning and de-provisioning user account entitlements (e.g., internal employee and personnel changes, custome access, suppliers' business relationships, or other third-party business relationships).

Mediclinic Software has ways you can control the software to customise it for your own purposes. You run your business your way.

We are an SAAS (Software As A Service) **supplier** and have many user roles and functions allocated at various times for our staff and programmers to access our software and servers. Over time you will get to know us and who we use. These people and positions may change time to time.

OTHER USER REQUIREMENTS

Some users may request we provide API or links to 3rd parties to enable better features for that client. Mediclinic Software will facilitate what we can that is legal and always complies with current legislation in place. We understand you may need extra Accounts Integrations or Marketing.



info@mediclinic.com.au

<https://mediclinic.com.au> TEL: 61 3 9947 1981

info@mediclinicsoftware.de

<https://mediclinicsoftware.de> TEL: 49 6925 7377 482

CAN I ASK YOU TO PROVIDE LINKS TO OTHER SERVICES I MAY WANT TO USE?

WE WILL NOT LINK ANY FACEBOOK OR GOOGLE DATA MONITORING PROGRAM TO OUR SOFTWARE or any API that had direct access to any data that may be transferred out of the country or region of operation. We may elect to TRANSFER data to these suppliers but the data we may transmit is on your request only and only in writing and only if that data we transmit is not against any current legislation. For example, we may transmit an address of your clinic or a provider name to GOOGLE ADS so your clients may book online or pay or receive an SMS or email.

If you make a request of us that we deem may be a security issue or to access data or for any other purpose, we may deny your request.

WE MAY MAKE CHANGES FOR YOU.

All changes and suggestions are to be done through the clients appointed representative and Mediclinic Software will do our best to ensure a rapid implementation of any request. Any requests not approved by the authorised client representative will not be implemented.

DATA PROTECTION OFFICER

In compliance with GDPR, HIPAA and Australian Government requirements our Data Protection Officer is **Natthapon Wongyai** and may be contacted at security@mediclinicsoftware.de

DATA COMPLIANCE AND WHERE YOUR DATA IS STORED

As we operate in many countries and countries have various rules and regulations on data protection, we use the standards set that are from the highest regulations from any country and we apply those as a minimum standard, always trying to exceed those standards. Your data is always stored on a server that complies with the legislation of the government of your country and on a server that always complies with the laws of your country.

At no time does your data ever leave to get stored in any other country than where we state hereunder. We also always maintain compliance with the various government legislation and laws and policies for the use, storage and dissemination of HEALTH DATA. To comply with relevant laws, we have licenses and signed agreements with relevant Government agencies in place where applicable.

AUSTRALIA & NEW ZEALAND – Your data is stored on Microsoft AZURE – Central Regions Servers which are the servers used for Critical Government Infrastructure for New Zealand and Australian Governments. We currently Hold agreements of compliance with The Australian Government Cyber Security Division of the Department of Human Services.

We comply with the various laws that are applicable to the various subsets of our software including SMS, Emails, Marketing internally by our clients and Cyber Security.

EUROPE and GERMANY

Microsoft AZURE (Munich as from January 2020) but currently in Netherlands - Amsterdam.



info@mediclinic.com.au

<https://mediclinic.com.au> TEL: 61 3 9947 1981

info@mediclinicsoftware.de

<https://mediclinicsoftware.de> TEL: 49 6925 7377 482

UNITED KINGDOM

London

UNITED STATES & CANADA

Iowa / Illinois/ Texas (these are the Secure servers for health Data)

ASIA & All other countries

Singapore

(These locations may change as needs and security compliances change from time to time.)

At all times we undergo continual testing and monitoring of laws and policies in place from time to time working with our Government Agencies in this regard. At all times we are compliant with all Privacy Policies and Data policies as well as financial and telecommunications laws as may be applicable to our software. We employ anti-spam and anti mass-marketing procedures for non-commercial activities. Where any conflict may occur we employ COMMON SENSE and employ procedures that maintain compliance as is expected.

WHO HAS ACCESS TO MY DATA AND HOW?

All staff of Mediclinic Software and the various parts of the companies that comprise Mediclinic Software may at times have access to your data and documents. All Mediclinic Staff are vetted for Security compliance and trust. This may be to enable us to assist you with enquiries, use and to help you use our software. At any time, your data is not sent outside of the country where we have stated it is stored for your region. Only the part of the data you and our team member may be accessing is shown on a screen for use. It is never downloaded.

EXCEPTION TO THIS RULE Sometimes our programmers may need to download parts of your data to rectify, assist or benefit you and they may be overseas. If this is done, you will be notified prior to this being done and we will always ask in writing or email for your permission. The permission must come from your person appointed by you as The Authorised person to do this which we will hold in our records system. Once the task has been completed the data will be destroyed.

HOW WE PROTECT YOUR DATA AND YOU

Mediclinic is proud of our security systems and the way we encrypt our data. It is important to know that whilst we would love to tell you every way, we protect you, we cannot. If we do, we open ourselves and you – to bad actors in the cyber area who will try to circumvent our protections.

We currently use DIGICERT HTTPS SSL encryption in the browser. We transmit your data encrypted to secure servers. Whilst on those servers your data is encrypted and remains encrypted whilst at rest. We encrypt your data at least 8 times. We also employ various other security methodologies in AZURE CENTRAL REGIONS SERVERS unique to CENTRAL



info@mediclinic.com.au

<https://mediclinic.com.au> TEL: 61 3 9947 1981

info@mediclinicsoftware.de

<https://mediclinicsoftware.de> TEL: 49 6925 7377 482

REGIONS SERVERS. We also configure data storage in a way we believe is unique to us which will also assist in securing your data.

Mediclinic Software is a CLOUD software solution operating in Secure, Government approved servers. We may use mirrored IP addressing and port disclosure for you to access your data and as such, anything you wish to access must always come through our software and you cannot add anything to our software without us knowing or adding this for you.

We also break your data up and store it on several servers always encrypted. For example, the name is one set of encryption, the date of birth another set and address another and so forth. No single person is stored as one single data set.

Currently we use AES 512 SSL Encryption which is currently the highest standard available and as these increase, we will make automatic adjustments keep up to date. Some, Mediclinic Staff will have access to all client data bases as the need to assist clients with various tasks. Clients will only have access to their data for their purposes.

In addition to this we are subjected as part of our agreements with Governments to their own systems testing including data breach protection and systems penetration testing which is performed randomly so we are never aware.

WE USE SECURITY KEYS & COOKIES

We use security keys which are used by the software to piece together your data in a complex array of data calls, so that we may deliver to you and keep your data safe and secure. We use various and multiple keys stored on separate servers using a unique procedure to match and extract and compile data for you. No client has access to or can change or make their own keys and these are stored on various Secure Servers within the AZURE Central Regions network and never on the same servers as the data of any client. We use multiple key structures using Azure so various parts of any client data are accessed by keys for that data set but not all of the data so any intrusion will result in data that is totally unreadable and unusable. This is done as a failsafe for the ultimate in data safety as per the highest of industry standards set out by Military Cyber Security experts.

We may use all or any of these types of Security keys.

*Super Key *Minimal Super Key *Candidate Key *Primary Key *Unique Key *Alternate Key

*Composite Key *Foreign Key *Natural Key *Surrogate Key

We do not advertise where and how we generate these keys to assist in ensuring total security compliances.

We also use cookies which we must in some countries advise you that we do. This is so we can provide services to you.

REDUNDANCY PROCEDURES FOR EMERGENCIES

Mediclinic Software has to be able to ensure you the client can access your data at all times. We are a global supplier of software and as such we use trusted partners such as Microsoft Azure (Government servers) and their partners who often are contractors but PREFERRED



info@mediclinic.com.au

<https://mediclinic.com.au>

TEL: 61 3 9947 1981

info@mediclinicsoftware.de

<https://mediclinicsoftware.de>

TEL: 49 6925 7377 482

suppliers. One of these suppliers is SAASPlaza, a company we use to maintain our servers on behalf of Microsoft. In the extraordinary event that we at Mediclinic Software are unreachable, you the client may reach or be contacted =by one of these suppliers. It is only in an extraordinary event this will have any need and you will automatically be contacted. For this purpose these suppliers who are not staff of Mediclinic Software may obtain access to your data files and documents but only for the purpose of assisting you. **At no time can they read or decipher the encrypted files we have made for you.**

DATA BREACH AND SECURITY INCIDENTS & HOW WE REPORT

Mediclinic Software maintains metadata for ours and your security. At times and without disclosure, we may log all user name and logins, Geolocation, IP locations, device used and operating system, browser type, time date and place and some metadata on device location and some other information for the purpose of verification of the user and permissions set by the client for that user.

We also restrict some countries from seeing or accessing our servers or websites.

Should we ever have the unfortunate situation of any data breach of any kind we have employed back end operations to ensure immediate notification to our appropriate staff and programmers. Should there be any breach of any kind we are legally compelled to notify Government and we will of course notify our client- YOU within 6 hours of us being alerted.

CLIENT NOT TO INITIATE SECURITY OR BREACH TESTING AT ANY TIME. Mediclinic Software **PROHIBITS** any client from initiating any security testing of data we hold whether or not the client insists this is their right. Should any client initiate any testing of any kind of our security features or data integrity features and or services Mediclinic Software will initiate a chargeable, non-negotiable and immediately payable and we have the right to direct charge any card or bank account you have nominated, a **fee of AUD 10,000** which is a strict part of our Terms of use.

As a part of our security policy we undergo regular testing such as penetration and other hacker simulations. We also prevent brute force attacks by limited the number of times a person can log in, where they can log in or try to reset username or password. After a certain number of failed attempts, then the client site administrator or a MEDICLINIC SUPPORT person needs to be contacted to have access restored. We will employ client KNOW YOUR CLIENT systems.

PLEASE BE ADVISED that using Mediclinic Software, we may log all events to a centralised log server to enable correct use verifications and incident reporting.

BACKUPS

Mediclinic Software employs state of the art solutions to backups which we test from time to time. We backup in 15 second intervals as a normal procedure with full back-ups done as a server snapshot every 15 minutes. The back-ups are done in an industry acceptable manner and we will hold all data in the back-ups as required under applicable laws which may be in



info@mediclinic.com.au

<https://mediclinic.com.au>

TEL: 61 3 9947 1981

info@mediclinicsoftware.de

<https://mediclinicsoftware.de>

TEL: 49 6925 7377 482

place time to time. If no law exists, then we will destroy all data within 30 days of the client's termination of service with us.

Should any client wish to have backups restored for testing or other purposes when there has been no identifiable breach of data or data loss, as that data is not corrupted in any way or manner then a one-time backup restoration **fee of AUD 1500** will apply. This is to cover the expenses of Mediclinic Software for any client who may wish to test their own data destruction procedures or staff sabotage.

Mediclinic Software has protected in-confidence procedures in place to prevent staff or any organisation client or internally from deleting information or data from any customer or client.

FAILSAFE PROCEDURES

Mediclinic Software has failsafe procedures in place to protect all areas of our business. It is well known that there are always actors in play trying to destroy, sabotage and delete and obtain data without consent and to try to hurt business operations. These bad actors can sometimes be internal or external.

We do not allow any API or other application or data function to access any part of our data that identifies a patient or a client or takes or removes data to another offshore location from where you operate. We do have PAYMENT access gateways but that data we allow to be transmitted at your request is so limited there is no breach of security. there is no higher security than what we employ. We export what data set is required only for the purpose of a single transaction. We send data that needs 3rd party applications to a separate server so no data or API can access our servers without us knowing. This prevents any Malware, advanced persistent threat or a network attacks, SSL or SQL injection, man in middle attacks, XSS and other attacks as well as "bad actor" attacks by other known government countries and hackers.

Mediclinic Software has source codes of our products and essential business separational elements that are only disclosed on an AS NEED TO KNOW BASIS. Not every person within our organisation can access every part of the company's source code or business elements. We have a TEAM that comes together, and you can rest assured this TEAM are owners and shareholders of the Group. We are a company operating in many countries of the world and as such we have procedures in place so in the event of any matter that is of an incident causing death or destruction to any part of the business we have plans and procedures in place to ensure viability and continual operations.

DEPROVISIONING OF USER OR CLIENT ACCESS

When you the client of Mediclinic Software decides to leave us, you can rest assured we will not use or hold your data unless required by law. PLEASE REMEMBER IT IS NOT UP TO US TO ENSURE any mandatory requirement you may have under your own professional body or government requirement. You may elect to reinstate any deactivated user account at any



info@mediclinic.com.au

<https://mediclinic.com.au>

TEL: 61 3 9947 1981

info@mediclinicsoftware.de

<https://mediclinicsoftware.de>

TEL: 49 6925 7377 482

time. This is in your control. **If you ask us to delete your data there is no way we can recover what you ask us to delete.**

WHAT CAN YOU STORE & ARE THERE LIMITS?

Mediclinic Software allows you to store any file type of your choosing and any limit of data size.

We do not allow you to open any file or documents on our server as that must be retrieved and downloaded to your user device and opened there. This ensures no malware or other infection process is placed on our servers. Whilst we employ security and anti-virus and other procedures, we also always try to ensure you as a client never infect any of yours or our databases.

TERMINATION OF AGREEMENTS

Mediclinic Software acknowledges that DATA IS ALWAYS YOURS. As long as all accounts are paid up to date and in full. We will usually deliver all saved files to you in the formats you have saved them, and data is exported usually in CSV formats to you.

MEDICLINIC SOFTWARE OPERATES EXCELLENT CUSTOMER SUPPORT. You can call us from anywhere anytime or email us. We have ONLINE support where we can show you on your device where to go and what to do. We have people working 6 days per week Monday to Saturday **18 hours a day, 365 days every year.** Most times we have a person allocated for your enquires EMAIL ONLY on a Sunday. Should any of your team have an issue no matter how small it may seem we are here to help and show them how to get the best from our software.

We pride ourselves in customer support and excellence of Service provision.
