

## **Medisonal Clinic Privacy Policy: How we handle your Personal Data**

### **About Us**

The Medisonal Clinic is a virtual, independent provider of private healthcare and education. In order to deliver healthcare services to our patients and receive payment for those services, we need to process some personal information about you (“personal data”), including information concerning your health. The Medisonal Clinic is therefore a “data controller”. This means that we exercise overall control over the personal data being processed through the determination of means and purposes of processing, and are ultimately in charge of and responsible for the retention and use of your data. In the event that another individual or organisation is the controller of your data, we will inform you.

At the Medisonal Clinic, we are dedicated to safeguarding and respecting your personal information. Our Privacy Policy provides a comprehensive explanation of the personal information we may gather from you and how it could be used. We advise you to carefully read through this Privacy Policy.

Our Data Protection Officer can be contacted at [thomas@medisonalclinic.com](mailto:thomas@medisonalclinic.com)

### **What data we collect**

Depending on your interactions with us, we may require specific information from you for various purposes. Our data collection is designed to be minimal, and we guarantee that only those with a legitimate need to access your information will be allowed to do so.

The personal data we may collect and process includes your name, contact details such as email address, home and mobile phone numbers, and address. If provided, we may use this information to contact you, which could involve emails, text, or voicemail messages, unless you indicate otherwise. We may also collect your date of birth, gender, and marital status, as well as information on your dependants, next of kin, and emergency contacts.

Additionally, we may gather data on your nationality, entitlement to treatment in the UK, and equal opportunity monitoring information, including ethnic origin, sexual orientation, health, religion or belief, and genetic data.

Concerning healthcare services, we will obtain contractual and financial information, such as the terms and conditions of your contract with us and your bank account and national insurance number if you are a self-pay patient or if a third party is responsible for payment of invoices/bills relating to your care. We will inform you beforehand if we intend to take payment from your credit or debit card. Health-related data may include your past and current medical records, information on medical or health conditions, including disabilities requiring reasonable adjustments, and details of medical or health conditions within your family.

We may also collect data related to our performance improvement, such as information on how you use our website, and feedback received from surveys, complaints, and claims.

If you are employed by the Medisonal Clinic, we may collect various personal data related to your employment. This may include your bank account details and national insurance number. We may also need to obtain information about your nationality and entitlement to work in the UK, as well as details of your work schedule, including working hours and attendance.

In addition, we may collect data on your periods of leave, including holiday, sickness absence, family leave, and sabbaticals, and the reasons for the leave. We may also keep records of any disciplinary or

grievance procedures you have been involved in, including related warnings issued to you and correspondence.

Furthermore, we may evaluate your performance through appraisals, performance reviews, ratings, and performance improvement plans, as well as related correspondence. We may also collect information about any medical or health conditions you have, including disabilities that require reasonable adjustments by the organisation. Additionally, we may gather information about any criminal record you may have and the COVID-19 status, vaccination status, and symptoms of you or anyone in your household.

If you are a healthcare professional at the Medisonal Clinic, we may collect personal data related to your provision of healthcare services to our patients. This may include information about your nationality and entitlement to practice in the UK, medical or health conditions, and vaccinations, including details on your COVID-19 vaccination status. We may also obtain data on whether you have a disability that requires reasonable adjustments from the organisation.

Additionally, we may gather information about the systems and services you utilise to provide care to our patients, as well as data received in response to any complaints or claims.

## **How we lawfully process your personal data**

We use your data for various purposes, ranging from obtaining your consent to send news and updates about us to fulfilling our legal obligations as a healthcare provider under English law. This requires us to have certain information about those we care for, including the following:

**Admitting you as a patient, assessing and providing medical care, and consulting with your clinician.** We may process your contact and demographic information, as well as special category data, to deliver our healthcare services.

**Protecting your or another person's vital interests.** We may process your personal or special category data if your life is at risk.

**Handling your queries or investigating complaints.** We may use your identity, contact, financial, transaction, payment, and/or special category data to respond or investigate, depending on the nature of your query or complaint.

**Obtaining your feedback, conducting analysis or evaluating our services.** We may use your contact, demographic, and/or special category data, under the legal grounds of legitimate interests or explicit consent.

**Ensuring ongoing care.** We may share information about your medical condition or diagnosis with your referrer, the NHS, international medical service, or other independent healthcare providers, for our legitimate interests and to ensure the ongoing provision of your care.

**Enabling payment/treatment authorisation, managing your account, and/or handling insurance claims.** We may share your basic identifiers, demographics, and/or medical reports with your insurer and/or third-party sponsor. This is necessary for our contractual obligations and the management of our healthcare system.

**Processing payment for your medical care.** We may process your payment details and other financial information, but we will not store your payment card details and instead use specialised third-party payment processors.

**Managing and maintaining our IT systems, and administering and protecting our business.** We may process your identity, contact, and technical data for troubleshooting, data analysis, testing, systems maintenance, and reporting, under our legitimate interests and legal obligations.

**Conducting clinical research.** We may use your identity, contact, demographic, and/or special category data with your explicit consent. We may use anonymised data for research, education and service development purposes, this will have no personally identifiable information included.

**Submitting data to national health initiatives or registries.** We may share your personal and/or special category data with national and other professional research or audit programs and registries where we are legally required to, where it is necessary for public interest or for our legitimate interests, or with your explicit consent.

**Assisting in protecting the public against dishonesty, malpractice, or other seriously improper behaviour.** For example, investigating complaints, clinical concerns, regulatory breaches, or investigations. Where personal data identifying you is not required, we will avoid using it as much as possible and may either anonymise the data or obfuscate your details. If we are subject to regulatory bodies, such as the Care Quality Commission, we are obligated to share data with them to investigate matters.

If you have any further queries, please contact our Data Protection Officer at [thomas@medisonalclinic.com](mailto:thomas@medisonalclinic.com) or your Consultant.

### **Where we get personal data**

In principle, we obtain your personal data directly from you, your consultant or a referring body. In the rare event that we receive information from a third party such as your General Practitioner (“GP”), NHS Trust, independent healthcare provider, insurer, international medical service, or family member, we will inform you before or during your interaction with your care team.

### **How we might share personal data**

In order to protect your privacy, we make every effort to limit sharing your personal data with third parties outside of the Medisonal Clinic. However, in certain situations, it may be necessary to provide access to your data to others. Some examples of third parties we may share your data with include:

- Consultants who are responsible for your care and treatment, including our Multidisciplinary Team (“MDT”).
- Suppliers or collaborators who assist us in providing you with services, such as 3D prosthetics or IT support.
- External healthcare providers including your General Practitioner (GP) where we believe this to be necessary to enhance the quality of your care. Let us know if you do not wish us to share information with your GP.

- Regulators, authorities, or government bodies who may require access to your data to resolve a complaint or for legal purposes.
- Professional advisers, such as external legal advisors, insurance companies, and medical experts, who may be involved in resolving a legal claim or dispute.
- National and professional research or audit programs and registries, approved researchers, and other healthcare organisations with your explicit consent or for legitimate interests.
- Third-party payment processors and delivery companies that assist in processing your payment or transportation needs.
- Third-party service providers for health, wellbeing, and patient safety analysis, such as storage and destruction of confidential information.

If possible, we will anonymise your data or use obfuscation techniques to protect your privacy when it is not necessary to include identifying information.

Please note that the NHS provides a national data opt-out digital service, which allows an NHS patient to opt out of their confidential patient information being used for research and planning. Find out more about the national data opt-out program on <https://digital.nhs.uk/services/national-data-opt-out>.

### **How long we keep personal data**

We will store your information in compliance with the retention periods set out in the Information Governance Alliance (IGA) Records Management Code of Practice for Health and Social Care (2016), the General Data Protection Regulation (2016) and the Data Protection Act (2018). However, we may retain your data for extended periods under the following circumstances:

- Retention for query resolution: We may keep your personal information for as long as necessary to address any inquiries you may have.
- Retention for potential claims: We may keep your personal information for as long as legally possible if there is a possibility of legal action against us.
- Retention for legal and regulatory obligations: We may keep your personal information after you have received healthcare services at our facilities to comply with our legal and regulatory requirements and obligations.

Generally, the following are the factors we consider when determining the appropriate period for retaining your personal data:

- The quantity, type, and sensitivity of your personal data.
- The potential risks of unauthorised use or disclosure of your personal data.
- The purposes for which we process your personal data and whether we can achieve those purposes through alternative methods.
- The relevant legal, regulatory, tax, accounting, or other requirements.

## **How we protect personal data**

It may not be possible to provide a comprehensive list of the specific measures we have in place to prevent unauthorised access, alteration, loss, or disclosure of your data. Nevertheless, we want to assure you that we are dedicated to safeguarding your data to the highest possible standards while it is under our care.

We have implemented various measures to achieve this goal, including:

- The establishment of organisation-wide security and data handling standards.
- The implementation of IT technical controls that limit access to your personal information only to those who need it for legitimate business purposes, including our employees, agents, contractors, and other third parties.
- The implementation of physical security controls in our buildings and wards.
- The implementation of contractual controls with third parties to ensure their compliance with our data protection policies and standards.
- The provision of training and awareness programs for all our employees and consultants.
- The appointment of key personnel with specialised knowledge of Information Governance, Data Protection, and Cyber Security to ensure the protection of your data.

These are just a few examples of the measures we have put in place to protect your data. We will continue to assess and improve our security measures to ensure that we meet our commitment to protect your data to the highest possible standard.

## **Your rights regarding your personal data**

In situations where we use your information with your consent, you have a significant amount of control over how your data is used and shared by the Medisonal Clinic. However, there may be circumstances where we use your data due to a legal obligation or other legitimate reasons, which could limit your rights under Data Protection Laws. For instance, in cases where we need to share or use your data to save your life, only a few of the Data Protection rights may apply.

Below is a summary of all the Data Protection rights and how they apply to your interactions with us:

- The right to be informed about the processing of your personal data: you have the right to be clearly informed about the collection and use of your personal data, which includes our purposes for processing your personal data, our retention periods for that personal data, and who it will be shared with. We provide individuals with this privacy information at the time we collect their personal data from them, except if it is impossible.
- The right to access your personal data: You have the right to request access to the personal data that we hold about you through a data subject access request. We will fulfil this request in all circumstances, but there may be situations where we cannot provide you with certain information in order to protect the rights of others or to maintain legal privilege/confidentiality. If we are unable to provide you with some of the information requested, we will explain the reason for this in our response to your request.

- The right to have your personal data corrected if it is inaccurate and to have incomplete personal data completed: You have the right to rectify any incomplete or factually inaccurate personal data that we hold about you. It is important to note that this right only extends to factual information, and not to opinions or medical diagnoses. This right applies in all circumstances, but there may be situations where we cannot make retrospective changes to your record. If this is the case, we will provide an explanation as part of our response to your request.
- The right to object to processing of your personal data: You have the right to object to our processing of your personal data in the following cases:
  - When we are relying on legitimate interest and you believe that your fundamental rights and freedoms are being affected. However, we may have compelling overriding legitimate grounds for the processing.
  - When we are processing your data for direct marketing purposes.
- The right to restrict processing of your personal data: If you want us to stop processing your personal data, you have the right to request that we temporarily suspend its use. This can be done in the following circumstances:
  - You want us to check the accuracy of the data.
  - The use of your personal data by us is illegal, but you do not want us to delete it.
  - You require us to keep the data to establish, exercise, or defend legal claims, even if we no longer need it for other purposes.
  - You have objected to our use of your data, but we need to verify whether we have legitimate reasons to continue using it despite your objection.
- The right to have your personal data erased (the “right to be forgotten”): In some cases, we may not be able to fulfil your request if there are specific legal requirements that require us to retain your personal data. We will inform you of these reasons if they apply when we respond to your request. You have the right to request the deletion or removal of your personal data in the following situations:
  - We no longer need your personal data for the purposes for which we collected it.
  - You have exercised your right to object to the processing of your personal data, or you have withdrawn your consent to such processing.
  - We have processed your personal data unlawfully.
  - We are required by law to erase your personal data.
- The right to move, copy or transfer your personal data (“data portability”): You have the right to request that we provide your personal data to you or a third-party of your choice in a structured, commonly used, machine-readable format (such as an Excel spreadsheet or a Word document). Please note that this right only applies to electronic or digital information that you have provided to us with your consent or that we use to fulfil our contractual obligations to you.

- Rights in relation to automated decision-making including profiling: you have the right not to be subject to decisions made only through automated means, without any human involvement. This right applies where the decision has a serious impact on you, which includes but is not limited to significant legal effects.
- Right to withdraw consent: You have the right to withdraw your consent for the processing of your personal data at any time. You can do this by emailing our Data Protection Officer at [thomas@medisonalclinic.com](mailto:thomas@medisonalclinic.com).
- Right to lodge a complaint with the relevant authority: You can complain about any concerns you may have over how your data is being handled. This complaint can be lodged either with us or with the ICO.
  - To register a complaint with us please email our Data Protection Officer at [thomas@medisonalclinic.com](mailto:thomas@medisonalclinic.com).
  - To register a complaint with the ICO please visit their website at [www.ico.org.uk](http://www.ico.org.uk) or address a letter to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or call their helpline on 0303 123 1113.

#### **Find out more**

Further information concerning how we handle your personal data can be provided from our Data Protection Officer on [thomas@medisonalclinic.com](mailto:thomas@medisonalclinic.com).

Please note that this Policy may be translated into other languages on request.