Privacy Policy

Karidis is committed to protecting and respecting your privacy.

Karidis understands that your personal data is entrusted to us and appreciates the importance of protecting and respecting your privacy. To this end we comply fully with the data protection law in force in the UK ("Data Protection Laws") and with all applicable clinical confidentiality guidelines including those published from time to time by the General Medical Council.

This Privacy Policy sets out the basis on which we collect and process personal data about you including our practices regarding the collection, use, storage and disclosure of personal data that we collect from you and/or hold about you, and your rights in relation to that data.

Please read the following carefully to understand how we process your personal data. By providing your personal data to us or by using our services, website or other online or digital platform(s) you are accepting or consenting to the practices as described or referred to in this Privacy Policy.

For the purpose of Data Protection Laws, the data controller is Karidis, with registered address at: Karidis Clinic, 3rd Floor, Hospital of St John & Elizabeth, 60 Grove End Road, NW8 9NH

When we refer to 'we', 'us' and 'our', we mean Karidis.

What personal data may we collect from you?

When we refer to personal data in this policy, we mean information that can or has the potential to identify you as an individual.

Accordingly, we may hold and use personal data about you as a customer, a patient or in any other capacity, for example, when you visit one of our websites, complete a form, access our services or speak to us. Depending on what services you receive from us this may include sensitive personal data such as information relating to your health.

Personal data we collect from you may include the following:

- information that you give us when you enquire or become a customer or patient of us or apply for a job with us including name, address, contact details (including email address and phone number)
- the name and contact details (including phone number) of your next of kin
- details of referrals, quotes and other contact and correspondence we may have had with you
- details of services and/or treatment you have received from us or which have been received from a third party and referred on to us
- information obtained from customer surveys, promotions and competitions that you have entered or taken part in
- recordings of calls we receive or make
- notes and reports about your health and any treatment and care you have received and/or need, including about clinic and hospital visits and medicines administered
- patient feedback and treatment outcome information, you provide
- information about complaints and incidents

- information you give us when you make a payment to us, such as financial or credit card information
- other information received from other sources, including from your use of websites and other digital platforms we operate (apps) or the other services we provide, information from business partners, advertising networks, analytics providers, or information provided by other companies who have obtained your permission to share information about you.

Where you have named someone as your next of kin and provided us with personal data about that individual, it is your responsibility to ensure that that individual is aware of and accepts the terms of this Privacy Policy.

Where you use any of our websites, we may automatically collect personal data about you including:

Technical information, including the Internet protocol (IP) address used to connect your computer to the Internet, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform,

The data that we request from you may include sensitive personal data. This includes information that relates to the mental or physical health or racial or ethnic origin (which may include children's data). By providing us with sensitive personal data, you give us your explicit consent to process this sensitive personal data for the purposes set out in this Privacy Policy.

When do we collect personal data about you?

We may collect personal data about you if you:

- visit one of our websites
- enquire about any of our services or treatments
- register to be a customer or patient with us or book to receive any of our services or treatments
- fill in a form or survey for us
- carry out a transaction on our website
- participate in a competition or promotion or other marketing activity
- make payments
- contact us, for example by email, telephone or social media
- participate in interactive features on any of our websites.
- In the interests of training and continually improving our services, calls to Karidis and its agents may be monitored or recorded.

What personal data we may receive from third parties and other sources?

We may collect personal data about you from third parties;

We may be passed medical information usually in the form of a referral for the purposes of your treatment with Karidis or a third-party consultant;

Consultants may need to share your personal data and medical records with Karidis;

Insurance providers will pass Karidis personal data of patients who have commenced a claim and require medical treatment with Karidis. This will normally be in the form of a referral

and may consist of basic details e.g full name, date of birth, address, contact number and email address and the type of procedure/treatment they require.

How do we use your personal data?

Your personal data will be kept confidential and secure and will, unless you agree otherwise, only be used for the purpose(s) for which it was collected and in accordance with this Privacy Policy, applicable Data Protection Laws, clinical records retention periods and clinical confidentiality guidelines.

Sensitive personal data related to your health will only be disclosed to those involved with your treatment or care, or in accordance with UK laws and guidelines of professional bodies or for the purpose of clinical audits (unless you object). Further details on how we use health related personal data are given below. We will only use your sensitive personal data for the purposes for which you have given us your explicit consent to use it. Please note that, although we have set out the purposes for which we may use your personal data below, we will not use your sensitive personal data for those purposes unless you have given us your explicit consent to do so.

We may use your personal data to:

- enable us to carry out our obligations to you arising from any contract entered into between you and us including relating to the provision by us of services or treatments to you and related matter such as, billing, accounting and audit, credit or other payment card verification and anti-fraud screening
- provide you with information, products or services that you request from us
- provide you with information about products or services we offer that we feel may interest you. Unless you have consented to receive marketing communications by electronic means from us, by ticking the relevant box on the form on which we collect your data, we will only contact you by electronic means (e-mail or SMS) with information about products and services similar to those which you previously purchased or enquired about from us
- allow you to participate in interactive features of our services, when you choose to do so
- notify you about changes to our products or services
- respond to requests where we have a legal or regulatory obligation to do so
- check the accuracy of information about you and the quality of your treatment or care, including auditing medical and billing information for insurance claims as well as part of any claims or litigation process
- support your doctor, nurse or other healthcare professional
- assess the quality and/or type of care you have received (including giving you the opportunity to complete customer satisfaction surveys) and any concerns or complaints you may raise, so that these can be properly investigated
- to conduct and analyse market research
- to ensure that content from any of our websites is presented in the most effective manner for you and for your computer.

The security of your personal data

We protect all personal data we hold about you by ensuring that we have appropriate organisational and technical security measures in place to prevent unauthorised access or unlawful processing of personal data and to prevent personal data being lost, destroyed or damaged. We conduct assessments to ensure the ongoing security of our information systems.

Any personal data you provide will be held for as long as is necessary having regard to the purpose for which it was collected and in accordance with all applicable UK laws. Please click here for more information relating to retention periods.

Personal data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Where we transfer your personal data outside the EEA, we will ensure that there are adequate protections in place for your rights, in accordance with Data Protection Laws. By submitting your personal data, and in providing any personal data to us, you agree to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your information is treated securely and in accordance with this Privacy Policy.

All information you provide to us is stored securely. Any payment transactions will be processed securely by third party payment processors. Where we have given you (or where you have chosen) a password that enables you to access certain parts of our website, you are responsible for keeping that password confidential. We ask you not to share a password with anyone.

The transmission of information via the internet cannot be guaranteed as completely secure. However, we ensure that any information transferred to our websites is via an encrypted connection. Once we have received your information, we will use strict procedures and security features for prevention of unauthorised access.

At your request, we may occasionally transfer personal information to you via email, or you may choose to transfer information to us via email. Email is not a secure method of information transmission; if you choose to send or receive such information via email, you do so at your own risk.

Disclosure of your personal data

In the usual course of our business we may disclose your personal data (to the extent necessary) to certain third-party organisations that we use to support the delivery of our services. This may include the following:

- business partners, suppliers and sub-contractors for the performance of any contract we enter into with you,
- organisations providing IT systems support and hosting in relation to the IT systems on which your information is stored,
- third party debt collectors for the purposes of debt collection,
- delivery companies for the purposes of transportation,
- third party service providers for the purposes of storage of information and confidential destruction, third party marketing companies for the purpose of sending marketing emails, subject to obtaining appropriate consent.

Where a third-party data processor is used, we ensure that they operate under contractual restrictions with regard to confidentiality and security, in addition to their obligations under Data Protection Laws.

We may also disclose your personal data to third parties in the event that we sell or buy any business or assets or where we are required by law to do so.

Health information collected during provision of treatment or services

Sensitive personal data (including information relating to your health) will only be disclosed to third parties in accordance with this Privacy Policy. That includes third parties involved with your treatment or care, or in accordance with UK laws and guidelines of appropriate professional bodies. Where applicable, it may be disclosed to any person or organisation who may be responsible for meeting your treatment expenses or their agents. It may also be provided to external service providers and regulatory bodies (unless you object) for the purpose of clinical audit to ensure the highest standards of care and record keeping are maintained.

Medical professionals working with us: We share clinical information about you with our medical professionals as we think necessary for your treatment. Medical professionals working with us might be our employees, or they might be independent consultants in private practice. In the case of independent consultants, the consultant is the data controller of your personal data, either alone or jointly with us and will be required to maintain their own records in accordance with Data Protection Laws and applicable clinical confidential guidelines and retention periods. Where that is the case, we may refer you to that consultant to exercise your rights over your data. Our contracts with consultants require them to cooperate with those requests. In all circumstances, those individual consultants will only process your personal data for the purposes set out in this Privacy Policy or as otherwise notified to you.

External practitioners: If we refer you externally for treatment, we will share with the person or organisation that we refer you to, the clinical and administrative information we consider necessary for that referral. It will always be clear when we do this.

Your GP: If the practitioners treating you believe it to be clinically advisable, we may also share information about your treatment with your GP. You can ask us not to do this, in which case we will respect that request if we are legally permitted to do so, but you should be aware that it can be potentially very dangerous and/or detrimental to your health to deny your GP full information about your medical history, and we strongly advise against it.

Your insurer: We share with your medical insurer information about your treatment, its clinical necessity and its cost, only if they are paying for all or part of your treatment with us. We provide only the information to which they are entitled. If you raise a complaint or a claim we may be required to share personal data with your medical insurer for the purposes of investigating any complaint/claim.

The NHS: If you are referred to us for treatment by the NHS, we will share the details of your treatment with the part of the NHS that referred you to us, as necessary to perform, process and report back on that treatment.

Medical regulators: We may be requested – and in some cases can be required - to share certain information (including personal data and sensitive personal data) about you

and your care with medical regulators such as the General Medical Council or the Nursing and Midwifery Council, for example if you make a complaint, or the conduct of a medical professional involved in your treatment is alleged to have fallen below the appropriate standards and the regulator wishes to investigate. We will ensure that we do so within the framework of the law and with due respect for your privacy.

From time to time we may also make information available on the basis of necessity for the provision of healthcare, but subject always to patient confidentiality.

In an emergency and if you are incapacitated, we may also process your personal data (including sensitive personal data) or make personal data available to third parties on the basis of protecting your 'vital interest' (i.e. your life or your health).

We will use your personal data in order to monitor the outcome of your treatment by us and any treatment associated with your care, including any NHS treatment.

We participate in national audits and initiatives to help ensure that patients are getting the best possible outcomes from their treatment and care. The highest standards of confidentiality will be applied to your personal data in accordance with Data Protection Laws and confidentiality. Any publishing of this data will be in anonymised, statistical form. Anonymous or aggregated data may be used by us, or disclosed to others, for research or statistical purposes.

Independent Healthcare Providers – Performance Information

In the interest in providing comparable clinical outcome and performance data to the public across independent sector providers in healthcare, we – like all independent hospital operators – are required by law to provide activity data, including some personal data, as set out in more detail below, for publication by The Private Healthcare Information Network (PHIN).

PHIN is responsible for collecting, processing and publishing information on the quality and cost of privately-funded healthcare in the UK. The publication of this information is intended to:

provide GPs with reliable information to inform their decisions about which providers to choose

help future patients make informed choices about where to seek treatment

enable providers of care (hospitals and consultant clinicians) to improve the quality and safety of their services by better understanding their performance by comparison with other providers

to support regulator information to help identify any causes of concern

enabling them to target inspections and help ensure safer care for patients.

Providers must provide to PHIN with details of each episode of care, including a summary of each record of treatment including; the dates when each patient was in hospital, what treatment was carried out and by whom.

Providers are also required to provide: patient satisfaction survey data, Patient Reported Outcome Measures (PROMS) – patient reported health improvements following treatment and details of any adverse events relating to the patients treated.

Providers are required to provide each patient's NHS Number (England, Wales or Isle of Man) or CHI Number (Scotland) and a post code of residence. This information can only be used to identify an individual by an approved body (such as an NHS hospital) with access to information linking NHS Numbers with other personal details. PHIN securely submits the patient's NHS number and discharge date(s) to information authorities such as:

- for England, NHS digital;
- for Wales, the NHS Wales Informatics Service;
- for Scotland, the Information and Statistics Division;
- for Northern Ireland, the Health and Social Care Board; and
- for UK-wide mortality data, the Office of National Statistics.

PHIN will only disclose records of care and personal data to the non-departmental bodies/authorities identified above, as required by law or where there is an overriding public interest, and /or to investigate or prevent fraud.

Data Protection Laws give all individuals the right to make a 'Subject Access Request' to obtain a copy of any information that any organisation holds about them (as set out in more detail below). As PHIN cannot identify individuals from the data it holds, applicants would need to provide their NHS Number (or equivalent in Scotland or Northern Ireland) and further proof of identity in order to access any information held.

Marketing

If you have consented to our processing your personal data for marketing purposes, in accordance with this Privacy Policy, we may send you information (via mail, email, phone or SMS) about our products and services which we consider may be of interest to you.

You have the right to ask us not to process your information in this way at any time.

If you no longer wish to receive web based marketing information you can unsubscribe by emailing enquiries@karidis.co.uk. For non-web-based marketing information please write to: Marketing Department, Karidis clinic, 3rd Floor, St John & Elizabeth Hospital, 60 Grove End Road, NW8 9NH with a reasonable amount of notice, to give us time to update our systems. While the precise timings vary we generally ask that you give us at least 30 days' notice.

Accessing and updating your information

The law gives you certain rights in respect of the personal data that we hold about you. In addition to your right to stop marketing, detailed above, below is a short overview of the most commonly-used rights. It is not an exhaustive statement of the law.

- With some exceptions designed to protect the rights of others, you have the right to a copy of the personal data that we hold about you
- You have the right to have the personal data we hold about you corrected if it is factually inaccurate. It is important to understand that this right does not extend to matters of opinion, such as medical diagnoses. If any of your personal data has changed, especially contact information such as: email address, postal address and

phone number please get in touch with so we can ensure your personal data is kept up to date

- If you want to exercise your rights in respect of your personal data, the best way to do so is to contact us by email on kimberley@karidis.co.uk or to write to us for the attention of the data protection officer at the address below. In order to protect your privacy, we may ask you to prove your identity before we take any steps in response to such a request.

Data Protection Officer, ADDRESS

FAO: DPO/ Kimberley Moriarty
Karidis Clinic
3rd Floor
St John & Elizabeth hospital
60 Grove End Road
NW8 9NH

If you would like to receive this Privacy Policy in any other form please do contact our Data Protection Officer so we can endeavour to meet your requirements as soon as possible.

If you are not satisfied with how we handle your request, you can contact the Information Commissioner's Office on 0303 123 1113 or visit their website (http://www.ico.org.uk).