JAPAN GREEN MEDICAL CENTRE LIMITED
PRIVACY POLICY

This is the privacy policy for Japan Green Medical Centre Limited (**JGMC**). It explains how and why we use personal data, and what we do to ensure information is kept safe and secure in accordance with applicable data protection and privacy laws including the UK Data Protection Act 2018 (**DPA 2018**) and the UK GDPR (being the UK's retained law version of the General Data Protection Regulation 2016/679) (**Data Protection Laws**).

This policy explains:

1. Who we are, and how to contact us

We are Japan Green Medical Centre Limited, a limited company with registered number 02396001, having our registered office and main place of business at Japan Green Medical Centre Limited, 10 Throgmorton Avenue, London, EC2N 2DL, United Kingdom. We are registered as a data controller with the Information Commissioner's Office (**ICO**) with registration number Z483616X.

If you have questions about this policy or your personal data, please contact our Data Protection Team by writing to our office address or by emailing reception@japangreen.co.uk with the subject line "Data Protection".

For the purposes of Data Protection Laws, we are a controller. This means we are responsible for deciding how and why we use personal data, and for keeping it safe.

2. When we collect personal data

We collect personal data (meaning information which relates to an identifiable individual) in a number of ways. These are described in more detail below.

Personal data we collect from you

Often the personal data we hold is provided to us by the person it relates to, for example when someone:

- enquires about our services (for example, by telephone or email) or fills in a form on our website;
- registers to become a patient; or
- provides us with their contact details and asks to receive news or correspondence.

We also process personal data relating to our dealings with that individual, which can include:

- information (including sensitive health personal data) generated in the course of providing medical services;
- contact details included in correspondence;
- bank details relating to payments we receive;
- recordings of telephone consultations; and
- images and video from CCTV outside our clinic.

Personal data received from third parties

We are sometimes provided with personal data by third parties, including related individuals, insurance providers, third party medical practitioners and other healthcare service providers (including NHS trusts). For example:

- your information might be provided to us by a patient who has listed you as their next of kin or emergency contact;
- if you are an employee of a corporate client, your employer may provide us with personal data about you;
- if you are a patient with medical insurance, your insurer may provide us with personal data (for example, regarding your policy); and
- we may receive personal data from other medical practitioners or healthcare services (for example, test results from a laboratory, or records from a hospital that has treated you).

3. What personal data we collect and who it relates to

Depending on whether or not you are a patient, the personal data we collect may include:

- personal details and contact information (such as name, address, telephone and email address);
- health information (including medical records, details of treatments we have provided, clinical photography and images from ultrasounds, x-rays and scans, referrals to and from other healthcare providers, notes and reports about your health);
- recordings of external telephone calls, including with patients;
- information about relationships to others (e.g. details of family and next of kin);
- bank or payment card details;
- correspondence and communication between you and us;
- feedback or complaints you provide about our services;
- details of your employer, or insurance status; and
- CCTV images (see part 6 of this policy for further information).

We may process other types of personal data, including additional categories of "sensitive personal data", particularly in relation to our patients. This will include medical and health information, and may also include information about an individual's race or ethnicity, religious beliefs or sexual orientation. Please see section 5 of this policy for further details.

We also process personal data on individual contacts at businesses and other organisations (such as representatives of other care providers, service providers, or professional advisers). We use this information for the purpose of our legitimate interests in running JGMC and building relationships with suppliers and other organisations.

Children and vulnerable persons

Some of the personal data we collect and process relates to children or vulnerable adults. We take extra care to ensure that personal data relating to such people is protected. If we require consent for the processing of personal data and the relevant individual does not have sufficient capacity to provide consent (as may be the case for children under 16 and some vulnerable adults) we will ask for consent from a parent or guardian.

We have a Children's Privacy Policy which explains how and why we use personal data in age-appropriate language for children. A copy of this can be found on our website and hard copies are available on request.

4. Why we process personal data

We use personal data because we need for one or more of the following reasons:

- to provide healthcare services to an individual (for example, to perform a contractual obligation we owe that individual);
- in order to comply with legal and professional obligations (such as record-keeping requirements, permitting regulatory audits, or disclosing information where required by Data Protection Laws and other applicable laws);
- to pursue our legitimate interests in operating and promoting the success of our business (such as using personal data for staff training, or contact details for marketing purposes);
- to pursue the legitimate interest of providing a safe environment for patients and staff (by using CCTV); and
- in an emergency we may use personal data to protect the vital interests of our patients.

If we process sensitive personal data (typically in relation to patients and occasionally their families), this is usually because we need to in order to provide medical treatment or healthcare services. However, we may also use this information because:

- the individual has provided their explicit consent to our doing so;
- in an emergency, we need to do so to protect the life of someone who is unable to provide consent; or
- we need to in order to establish, exercise or defend a legal claim.

5. Patient health data

We process sensitive health data (which Data Protection Laws class as 'Special Category Personal Data') in connection with the health care services we provide. This may include:

(a) data concerning health;

(a) racial or ethnic origin data;

(b) genetic data; and

(c) data concerning an individual's sex life or sexual orientation.

In each case:

(a) such data are processed because the processing is necessary for:

(i) the performance of a contract with the data subject (Article 6(1)(b) UK GDPR) (i.e. a contract to provide health care and treatment) whilst the relevant individual is a patient.

(ii) our legitimate interests in operating a healthcare business, this includes complying with healthcare industry standards, staff training and (in the case of telephone recordings described in paragraph 6 of this policy) keeping records to ascertain the facts of a matter;

(iii) to comply with a legal obligation (Article 6(1)(c) UK GDPR) (such as a legal obligation to maintain health care records); and

(b) our additional condition for processing special category data is that the processing is necessary for health care purposes (Paragraph 2(1) Schedule 1, DPA 2018 and Article 9(2)(h) UK GDPR) including preventive or occupational medicine, the assessment of the working capacity of an employee, medical diagnosis and the provision of health care or treatment.

In accordance with section 11(1) DPA 2018, the processing of Special Category Data described in this Paragraph 5 shall only be carried out by or under the responsibility of a health professional (as defined in section 204(1) DPA 2018), or by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

6. Recording telephone calls

JGMC routinely records external telephone calls (incoming and outgoing) with patients, unless the patient has chosen to object to the recording and opt-out, which can be done easily by following the in-call instructions.

We record telephone conversations for the following purposes, which are in our legitimate interests in accordance with Article 6(1)(f) UK GDPR.

(a) Quality Assurance: to ascertain compliance with applicable regulations and related practices and procedures, including healthcare provider regulations.

(b) Fact checking: to establish the existence of facts relevant to JGMC's business and protect our staff and patients. For example if there is a complaint made by a patient of if a patient is verbally abusive towards a member of our staff.

(c) Staff Training: to ascertain or demonstrate the standards that are expected to be achieved by staff, for example, for quality control or staff training.

In addition to the content of the telephone call, we keep a log of the caller's number as well as the date and time of the call.

We are aware that telephone calls between patients and JGMC staff may include confidential health information of a very private nature, and we have taken extensive steps to ensure that patients' data protection rights are protected. In particular, we have done the following:

- Patients are given the ability to simply and easily opt-out of and object to call recording;
- The fact that calls are recorded is clearly notified to patients by in-call messages in English and Japanese;
- Recordings are automatically deleted after 30 days unless there is a compelling lawful reason for retaining them for longer (for example, a complaint by a patient or abuse towards JGMC staff);
- Recordings are stored in a secure encrypted format in a UK data centre. Access is strictly controlled and any access is logged and will only be permitted where absolutely necessary;
- We work with a specialist telecommunications service provider who has provided legally binding promises and guarantees of security to ensure your personal data is protected; and
- Recordings can be deleted on request in accordance with an individual's data subject rights under UK GDPR.

If you have any questions regarding our use of telephone call recording or wish to have a call recording deleted, please contact us by emailing reception@japangreen.co.uk or by calling 020 7330 1750.

7. Job applicants

We collect, store and use personal data about individuals who apply to join JGMC. This may include information:

- provided to us (such as in CVs, application forms, and through correspondence);
- provided during an interview;
- obtained from previous employers and referees;
- provided to us by recruitment agencies; and
- received as a result of our carrying out background checks (such as checks for criminal convictions with the Disclosure and Barring Service).

We may carry out a check for criminal convictions in order to satisfy ourselves that there is nothing in an applicant's history which makes him or her unsuitable for the role. We do this because working with us involves a high degree of trust (as our staff deal with vulnerable people and will have access to health data and other confidential information).

We only carry out criminal records checks and ask for references at the last stage of the application process, when making an offer of employment.

How we use applicant information

We use the personal data we collect to:

- assess an applicant's skills, qualifications, and suitability for a role;
- carry out background and reference checks;
- communicate with an applicant about the recruitment process;
- keep records related to our hiring process; and
- comply with legal or regulatory requirements.

We do all of this either because it is necessary in order for us to enter into a contract of employment or because we have a legitimate interest in ensuring an applicant is suitable for

a particular role. Without this personal data, we will not be able to process an application successfully.

If we need to process sensitive personal data about a job applicant, for example disability information in order to consider whether we need to provide appropriate adjustments during the recruitment process, we will ask for explicit consent to do this at the time at which we request the data.

Retention of applicant information

We normally retain personal data about unsuccessful applicant for between 3 and 6 months from the time we inform them of our hiring decision. We retain personal data for this period so we can demonstrate, in the event of a legal claim, that we have not discriminated against an applicant and that the recruitment process was fair and transparent. After this period, we will securely destroy the applicant's personal data. If we wish to retain personal data on file, in case future opportunities arise, we will contact the applicant and ask for his or her consent to do so.

If an applicant is successful, some of the personal data provided in the application process will be stored as part of the staff member's personnel file, and any unnecessary information will be securely destroyed.

8. How we use CCTV

We have CCTV at the entrance to our clinic in order to protect the security of our clinic and the safety of the people within it. We have a single CCTV camera located on the exterior of the building which records video images of persons entering and leaving the clinic. A notice is posted below the camera to ensure that people are aware of CCTV image recording.

Images recorded by CCTV are stored for a period of 30 days, after which they are automatically deleted. Access to CCTV images is restricted to designated staff, who will only view the recording where necessary. We only share CCTV with others in exceptional circumstances (such as requests from law enforcement) or if required by law (such as pursuant to a court order or data subject access request). If there is a possibility of recordings being made public (for example, to assist in the identification of an offender) we will consult with and take into account the wishes of any other persons who might be affected, although we will usually blur or disguise the faces of individuals where possible.

Our staff are required to comply with a strict policy regarding the use of access to CCTV, and we adhere to the guidance on video surveillance (including the use of CCTV) produced by the ICO which can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/video-surveillance/

9. Communications

We use personal data to contact people as part of the services we provide, and when we need to in order to operate our medical practice. For example, we may contact patients to remind them about an appointment or let them know their results are ready. We might do this through a phone call, text message, email or by post.

We will only contact you personally with email marketing communications if you have specifically asked to receive marketing.

We sometimes send emails to other companies and organisations without their prior consent. We do this in order to promote our services and build relationships. If we have contacted you like this, it is because we think these communications may be of interest or relevance to you (usually on the basis of our previous dealings with you or a recommendation from a third party).

You can change how you hear from us or unsubscribe from marketing at any time by clicking the “unsubscribe” link on any of our emails, or by emailing reception@japangreen.co.uk with the subject line “unsubscribe.”

10. Cookies and website visitors

We do not normally collect personal data about visitors to our website unless they choose to provide such information (such as by filling in a website form).

We collect anonymous information about visitors to our website in order to optimise and improve the website. This might include IP addresses, browser or device details and the connection type (e.g. the Internet service provider used). However, none of this information will by itself directly identify any particular user.

Cookies

Our website uses “cookies” to enhance your experience and enable certain functionality. Web browsers place cookies on hard drives for record-keeping purposes and sometimes to track information (such as repeat visits). You can choose to set your web browser to refuse cookies, or to alert you when cookies are being sent. However, if you refuse to allow cookies, this may interfere with your ability to use the site.

We use Google’s AdWords remarketing service. This means that if you visit our website, you may see adverts for JGMC when you visit other websites. This happens because Google places a cookie on your machine based on which pages you visit on our site, and then uses that cookie to show you relevant advertisements when you visit other sites. This remarketing process does not involve collecting or storing any of your personal data.

You can opt-out of Google’s use of cookies by visiting Google’s Ads Settings . Alternatively, you can-opt out of Google and third-party cookies by visiting the Network Advertising Initiative opt-out page.

Hyperlinks to other sites

Our website contains hyperlinks to third-party websites (such as private hospitals). We are not responsible for the content or functionality of any of those external websites. If an external website requests personal data from you the information you provide will not be covered by this policy. We suggest you read the privacy policy of any website before providing any personal data.

11. Recipients of personal data

Personal data you provide to us will be kept private and confidential, and we will not disclose or share it with other data controllers without your permission (for example, if you are a patient and an employer or insurer requests medical information about, we will only share this with your explicit consent). The only exception to this is where we are legally required to disclose personal data, such as where we are required to provide information to law enforcement, or pursuant to a request from a regulator or a court order.

We sometimes share personal data with third parties who provide services to JGMC. However, these service providers will only process personal data on our behalf, for specified purposes, and in accordance with our strict instructions.

We only use third party service providers who have provided sufficient guarantees that your personal data will be kept safe, and we always ensure there is a written contract in place which protects your personal data and prevents it from being used for any purpose other than providing services to JGMC.

12. How long we store personal data for

We only store personal data for as long as is necessary for the purpose(s) it was collected for, or for related compatible purposes (such as record keeping, in order to comply with legal and regulatory requirements and because information may be required if a claim later arises).

In the case of patients (and related individuals such as next of kin) we store personal data for the duration of the treatment. We will then store the information for the periods set out in table below.

Telephone recordings	30 days (unless there is reason to store the recording for longer)
CCTV recordings	30 days (unless there is reason to store the recording for longer)
Patients under age 17 at the date of treatment	Until the patient's 25th birthday
Patients aged 17 at the date of treatment	Until the patient's 26th birthday
Patients who have died before age 18	8 years from the patient's death
Patients treated by a GP	10 years from the last record entry
Obstetric, maternity, ante-natal and post-natal records	25 years
Cancer and oncology records, and records of long term re-occurring illnesses	30 years
Mental health records	Up to 20 years
Contraception, sexual health, family planning and genito-urinary medicine	Between 8 and 10 years for adults, depending on the type of treatment

Other types of record may be stored for different periods, and we adhere to the best practice retention recommendations contained within the Records Management Code of Practice for Health and Social Care. For further information and a detailed breakdown of our retention periods, please visit https://digital.nhs.uk/records-management-code-of-practice-for-health-and-social-care-2016.

In all other cases, we will determine the appropriate retention period for personal data by considering the amount, nature, and sensitivity of the personal data, the potential risk of harm from its unauthorised use or disclosure, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Once personal data is no longer required it will be securely destroyed.

13. How we keep personal data safe

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, damaged or destroyed, altered or disclosed. This includes both physical security measures (such as keeping paper files in secure premises) and electronic security technologies (such as device encryption and anti-virus protection).

We limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to strict legal and contractual confidentiality obligations.

We have put in place procedures to deal with any suspected personal data breach and will notify you, the ICO and any other relevant regulatory body of a breach when legally required to do so.

14. International transfers

We normally only store personal data within the UK. However, some of the third-party services we use from time to time may be provided by companies which are based elsewhere. Before using such service providers, we will take steps to make sure that any personal data they process on our behalf is adequately protected and transferred in accordance with Data Protection Laws, usually by one or more of the following methods:

- ensuring the recipient is in a country which provides adequate protection for personal data in accordance with Data Protection Laws;
- implementing appropriate safeguards such as requiring the recipient to enter into Standard Data Protection Clauses approved by the ICO; or
- Data Protection Laws otherwise permit us to make the transfer.

If you would like more detailed information on the measures and safeguards which we implement for such data transfers, then please contact us using the details set out in section 1 above.

15. Your rights as a data subject

Data Protection Laws provide you with certain rights in relation to your personal data. These are as follows:

- **The right to access your personal data.** This enables you to receive a copy of the personal data we hold about you.
- **The right to request correction or completion of personal data**. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **The right to request erasure of your personal data**. This enables you to ask us to delete or remove personal data (though this may not apply where we have a good, lawful reason to continue using the information in question). You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).
- **The right to object to processing of your personal data.** You can object to us processing personal data for legitimate interests purposes (this includes opting out of telephone recordings) or for direct marketing.
- **The right to restrict how your personal data are used**. You can limit how we use your information (primarily to storage or for use in legal claims).
- **The right to have a portable copy or transfer your personal data**. We will provide you, or (where technically feasible) a third party, with a copy of your personal data in a structured, commonly used, machine-readable format. Note this only applies to automated information we process on the basis of your consent or in order to perform a contract.
- **The right to withdraw consent.** If we are relying on consent to process your personal data you have the right to withdraw that consent at any time.

Responding

We try to respond to all personal data requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of

requests. Please also bear in mind that there are exceptions to the rights above and some situations where they do not apply.

We may need to request additional information from you to help us confirm your identity. This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you to clarify your request.

Fees for making a request

You will not normally have to pay a fee to access your personal data (or to exercise any of your other rights). However, we may charge a reasonable fee if your request is unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

How to make a request

If you want to exercise any of the rights described above, please contact our Data Protection. Team by writing to Japan Green Medical Centre Limited, 10 Throgmorton Avenue, London, EC2N 2DL, United Kingdom or emailing reception@japangreen.co.uk, clearly stating the nature of your request. JGMC can provide you with a template request form to assist you in making your request.

Your right to complain to the Information Commissioner's Office

You have the right to complain to the Information Commissioner's Office if you are not satisfied with our response to a data protection request or if you think your personal data has been mishandled. For further information on how to make a complaint, please visit https://ico.org.uk.

16. Updates to this policy

We will update this policy from time to time, so please check back. The current version will always be posted on our website. This policy was last updated on the 17 July 2023.

16. Children's Privacy Policy

"Children friendly" policy has been added to this "Privacy policy" as supplemental policy.