Patient privacy and confidentiality policy

Approved policy | Effective 22 November 2026 | Version 1.0

Our commitment

Blue Dental Care respects your privacy and the confidentiality of your dental care. This policy sets the standards our team must follow when collecting, using, sharing, storing and disposing of patient information. It covers NHS and private care and communications with the practice.

The practice and your contact

Blue Dental Care is a trading name of Shamila Limited, at 232 Stockwell Road, Brixton, London SW9 9SU. Prabakar, Manager, is the day-to-day contact for privacy questions, access requests and concerns. Email mail@bluedentalcare.co.uk or telephone 020 7274 3085.

The current ICO registration certificate records SIVASHANKAR SRI RANGANATHAN / BLUE DENTAL CARE, reference Z1377753, expiring 3 July 2027. ICO fee registration is not a certification of compliance.

Information used for care and administration

We use identity and contact details, medical and dental histories, clinical notes, radiographs and other clinical images, treatment plans, referrals, appointment information, payments, NHS declarations, correspondence and relevant communication or access needs. Information may come from you, an authorised representative or professionals involved in your care.

We use the information needed to assess and provide care, arrange appointments, communicate about treatment, manage payments and NHS administration, make appropriate referrals, provide support and reasonable adjustments, respond to complaints and meet applicable legal, professional and safeguarding duties. Please keep your details current. Without information needed for safe treatment or a required declaration, we may need to clarify matters before proceeding.

Lawful, limited and confidential use

The practice must identify and document a lawful basis for each use of personal information. Depending on the purpose and circumstances, the relevant basis may be a contract with the patient, a legal obligation, an NHS public task with a basis in law, or an assessed legitimate interest. A legitimate interest must not override a patient's rights and must not be used in place of the basis for an official public task.

Health information needs an additional legal condition. Necessary diagnosis, treatment and management of healthcare may use the healthcare condition in Article 9(2)(h), subject to professional confidentiality. That condition does not authorise unrelated use of patient information, such as general AI-model training.

Where consent is the basis for an optional use, it must be specific and freely given. You can withdraw that consent without affecting the lawfulness of earlier use. Consent to dental treatment is separate from the legal basis for keeping a clinical record. Staff must only access information needed for their work and must not browse records out of curiosity.

Privacy when you visit

Reception is open plan and has no private booths. We normally send an online medical-history form before your appointment and do not ask you to discuss your medical history at the reception desk. You can speak privately with your dentist in the surgery.

We also send the FP17 declaration before NHS treatment. If it has not been completed, reception may need to ask about exemption eligibility and arrange your declaration. Tell the team if you need a discreet way to discuss this or help completing a form. Staff must limit conversations and visible information in reception to what is necessary.

CCTV and telephone recordings

CCTV operates in public areas and telephone conversations with patients are recorded. These recordings are personal information and are subject to the same requirements for lawful purpose, necessity, security, limited access and appropriate retention as other patient information.

The practice must explain the purpose of recording, provide clear CCTV notices and tell callers about recording. Recording must be proportionate to a documented purpose. Access, copying and disclosure must be restricted to authorised people with a reason to use it. Contact Prabakar if you have a question about a recording or wish to request access; we may need to protect information about other people.

AI assistance and human oversight

If a clinician uses an AI assistant to help prepare notes, they will tell you at the start of the appointment and before capture. They must explain its use and give you an opportunity to raise concerns. If you do not want it used, tell the clinician; they must use an appropriate alternative for taking your notes. The clinician remains responsible for checking the record and for clinical decisions.

AI-assisted booking and communication must use only the information needed for the relevant task. You can ask for help from the practice team. No tool may be given patient information until its purpose, privacy information, supplier terms, access controls, retention and any transfer arrangements have been checked. Any separate supplier use, including model training, requires its own lawful justification; healthcare use must not be treated as blanket permission.

Sharing and service providers

Relevant information may be shared with clinicians involved in treatment or referral, dental laboratories, NHS bodies responsible for claims and administration, payment services, and providers supporting clinical records, booking, communications or recordings. Professional advisers, regulators, safeguarding bodies or other organisations may receive information where authorised or legally required. Sharing must be limited to what is needed and must respect confidentiality.

Where a supplier processes information on our behalf, the practice must use appropriate contractual and security controls. Any access or processing outside the UK must be assessed and supported by a lawful transfer arrangement. Patients must be given information about applicable transfers and how to obtain details of the safeguards; a supplier's marketing claim alone is not sufficient evidence.

Keeping and disposing of information

Retention must be decided by record type and documented. Our criteria are the purpose of the record, continuing care needs, patient age, applicable NHS, legal and professional requirements, and any unresolved complaint, safeguarding matter, claim or legal hold. A specific period already adopted for a record or system must be followed and explained to patients where relevant.

Clinical records: consider continuity and future clinical relevance, the patient's age at treatment, safeguarding needs, applicable retention requirements and the need to establish or defend claims. Do not delete a clinical record simply because a patient leaves the practice or asks to withdraw treatment consent.

Payment and NHS administration records: consider reconciliation, tax and accounting duties, NHS audit or recovery requirements and unresolved payment disputes. Complaint records: keep separately from clinical records and retain according to investigation, review, legal and safeguarding needs.

CCTV and telephone recordings: routine material must be kept for the shortest justified period for its documented purpose. Specific material may be preserved where needed for an incident, complaint, information request or claim, with restricted access and a review of continuing need. Do not keep all recordings indefinitely.

AI audio and transcripts: distinguish temporary source material from the clinician-checked clinical record. Keep source material only where necessary for the stated purpose and for a documented period, considering verification, correction and any incident or legal hold. Do not assume that a supplier automatically deletes it. The final clinical record follows the clinical-record retention rules.

When retention is no longer justified, information must be securely deleted, destroyed or irreversibly anonymised, including appropriate management of copies and backups. Confidential paper must be disposed of securely.

Your information rights

You can ask to access and receive a copy of your personal information, correct inaccuracies and exercise other rights where the legal conditions apply, including erasure, restriction, objection and portability. Some rights are limited where records must be retained or information is needed for care, legal duties or claims. We will explain any applicable limitation.

Contact Prabakar at mail@bluedentalcare.co.uk or write to the practice. You do not have to use a particular form. We may need to confirm your identity or clarify the request. We will respond within the applicable legal time limit, normally one month, and explain any permitted extension. Please tell us if you need an accessible format or communication support.

Concerns, complaints and review

For a complaint about your information, email complaints@bluedentalcare.co.uk. We will investigate and explain the outcome. You can also complain to the Information Commissioner's Office at ico.org.uk/make-a-complaint/ or telephone 0303 123 1113. Making a complaint will not itself affect your care.

The Manager coordinates this policy, staff awareness and review with the responsible data-protection and clinical leads. The policy must be reviewed when services, information systems or legal requirements change and at least at the next review date.

Approved by Prabakar, Manager. Effective 22 November 2026. Next review 22 November 2027.