SUBJECT ACCESS REQUEST (SAR) POLICY GROSVENOR HOUSE SURGERY

1. Purpose
    - To set out how the practice will handle Subject Access Requests (SARs) in line with UK GDPR and the Data Protection Act 2018.
    - To protect patients' confidentiality while ensuring timely, lawful access to personal data.

2. Scope
    - Applies to all SARs for personal data held by the practice in any format (electronic, paper, audio).
    - Covers requests from data subjects, their authorised representatives, and parents/guardians where applicable.
    - Excludes requests for deceased patients' records (handled under Access to Health Records Act 1990).

3. Roles and responsibilities
    - Data Controller: The GP partnership.
    - Senior Responsible Officer/Practice Manager: Day-to-day oversight of SARs.
    - Data Protection Officer (DPO): Advises on compliance and complex cases; reviews DPIA impacts.
    - All staff: Must recognise SARs, escalate promptly, and follow this policy.

4. How to make a SAR
    - Accepted channels: written letter, secure email, practice webform, or verbal request (we will document and confirm).
    - Identity verification: We will request one photo ID and one proof of address (e.g. passport/driving licence/utility bill) where needed to confirm identity or authority.
    - Third-party/representative requests: Must include signed authority or proof of parental responsibility/court order as relevant.

5. Timescales
    - Standard response time: within one month of receiving the request, or from identity/authority confirmation if required.
    - Extensions: May extend by up to two further months for complex or multiple requests; we will inform the requester within one month with reasons.
    - We will acknowledge all requests promptly and provide an indicative timeline.

6. Fees
    - No fee for standard SARs.
    - Reasonable fee may be charged for manifestly unfounded/excessive requests or for additional copies; we will notify in advance.

7. What will be provided
    - A copy of the personal data we process about the requester, including:
        - Health record entries (prospective and retrospective as applicable), correspondence, results, coded data, and relevant free text where appropriate.
        - Supplementary information required by law (purposes, categories, recipients, retention, rights, sources).
    - Format: Secure electronic (preferred, e.g. PDF/CSV) or paper copy if requested and feasible. We will ensure data is provided in a structured, commonly used, machine-readable format where appropriate (data portability only applies where lawful basis is consent/contract).

8. Redactions and exemptions
    - We will not disclose:
        - Third-party identifiable information without their consent unless reasonable to do so.
        - Information that could cause serious harm to the physical or mental health of the data subject or another person.
        - Legally privileged or legally restricted information.
    - A GP or appropriate clinician will review any potentially harmful clinical content prior to disclosure.
    - We will document redaction decisions and provide explanations of withheld information where we can.

9. Verification, safeguarding and special cases
    - Vulnerable patients: We will consider safeguarding risks, coercion, or domestic abuse concerns before enabling access (including online record access). Mitigations may include restricting access, face-to-face verification, or providing a summary.
    - Children/young people: Assess Gillick competence and best interests. From the point a child is competent, they may make their own SAR; parental access may be limited accordingly.
    - Representatives (e.g. solicitors/insurers): We will confirm authority and scope; we will not provide general open access to the entire record where not necessary and proportionate.
    - Deceased patients: Requests are handled under separate process (Access to Health Records Act 1990).

10. Records location and searching
    - We will make reasonable efforts to search all systems and formats where personal data is held, including clinical systems, document management, and archived records.
    - We may ask the requester for details to help us locate specific information efficiently.

11. Security of disclosures
    - We will use secure methods for transmission (e.g. encrypted email, secure portal, or recorded post). We will confirm preferred method and contact details with the requester.
    - In-person collection requires ID.

12. Refusing a request

- We may refuse or partially refuse a SAR if it is manifestly unfounded or excessive, or where exemptions apply. We will provide reasons and information on how to complain.

13. Complaints and escalation
    - Practice-level: Contact the Senior Responsible Officer/ Practice Manager/ GP Partners
    - External: Information Commissioner's Office (ICO) — ico.org.uk/concerns or 0303 123 1113, ICO, Wycliffe House, Water Lane, Cheshire SK9 5AF.

14. Training and awareness
    - All staff will receive periodic training on recognising and handling SARs, redaction principles, and verification.
    - The practice will maintain FAQs/standard operating procedures for staff.

15. Data breaches
    - Suspected personal data breaches related to SAR handling will be escalated via our incident process. We will notify affected individuals and regulators where legally required.

16. DPIA and related documents
    - This policy should be read alongside our DPIA for online records access, our confidentiality policy, and our retention policy.
    - Plans and mitigations may be shared with our ICB and the ICO alongside the DPIA where appropriate.

17. Review
    - This policy will be reviewed annually or after significant legislative or operational changes.

18. Patient information: How to make a SAR
    - You can request a copy of your personal information by contacting Grosvenor House Surgery. We may ask for ID to keep your information safe. We usually respond within one month. Further guidance about your rights is available from the ICO at ico.org.uk.