SABA
HEALTH CLINIC

Summary of Your Data Protection and Privacy Rights

SABA Health's Commitment to You

We take your privacy and the security of your personal information very seriously. This summary explains how SABA Health looks after your data, following the UK's data protection law (UK General Data Protection Regulation - UK GDPR and the Data Protection Act 2018).

Our main goal is to process your information lawfully, fairly, transparently, and securely.

What Information We Collect

We process two main types of information about you:

- **Personal Data:** Any information that can identify you, such as your name, address, and contact details.
- **Special Category Data:** This is sensitive health information that needs extra protection, such as details about your health, medical history, genetic data, or ethnicity.

Data Processing means anything we do with your data, including collecting it, storing it, using it, sharing it, or deleting it.

Why We Use Your Data (Lawful Basis)

We must have a valid legal reason to use your data. At SABA Health, we use your data primarily for:

- **Providing Health Care and Treatment:** This is the core reason for processing your data.

- Legal Requirements: To meet our obligations under health and social care laws.
- Contractual Needs: When necessary to fulfill an agreement with you.
- Special Category Data: We process your sensitive health data specifically for the provision of health care, which is a special exemption under the UK GDPR.

How We Keep Your Data Safe

We follow seven key Data Protection Principles to ensure your data is handled correctly:

1. **Lawful, Fair, and Transparent:** We use your data legally and openly.
2. **Purpose Limitation:** We only use your data for the specific purposes we told you about.
3. **Data Minimisation:** We only collect and hold data that is necessary and relevant.
4. **Accuracy:** We ensure your data is correct and up-to-date.
5. **Storage Limitation:** We only keep your data for as long as it is needed.
6. **Integrity and Confidentiality (Security):** We keep your data secure and protected.
7. **Accountability:** We take responsibility for following all the data protection rules.

Security Measures

SABA Health ensures:

- **Electronic Data:** Stored on secure, encrypted systems. Access is limited by passwords and based on what a staff member needs to do their job (role-based access)
- **Paper Records:** Stored securely with controlled access.
- Your data is protected from being lost, misused, or accessed by people who are not authorised.

When and How We Share Your Data

Your personal data will only be shared in specific, lawful situations:

- **Legal Requirements:** If the law demands it.
- **Consent:** If you have given your consent (where appropriate).
- **Authorised Third Parties:** With other authorised organisations (like a specialist hospital or a testing lab) under formal data-sharing agreements that ensure they also protect your data.
- Any sharing of your data must be lawful, necessary, and properly documented.

Your Rights Over Your Data

You have important rights regarding your personal information, and we will handle all requests within the legal timeframes:

- **Right to Access:** You can ask for a copy of the personal data we hold about you.
- **Right to Correction:** You can ask us to correct any inaccurate information.
- **Right to Erasure (Right to be Forgotten):** You can ask us to delete your data in certain situations (e.g., if we no longer need it).
- **Right to Object:** You can object to us processing your data.
- **Right to Restriction:** You can ask us to limit how we use your data.
- **Right to Data Portability:** In some cases, you can ask to receive your data in a format that allows you to easily transfer it to another organisation.

What to Do If There Is a Data Breach

A data breach means any loss, theft, unauthorised access, accidental disclosure, or cyber security incident involving your data.

If a breach happens:

- It must be **reported immediately** to the Medical Director (Dr. Syed Sheik).
- It will be **investigated promptly**.
- We will report it to the Information Commissioner's Office (ICO) if the law requires it.
- It will be managed according to SABA's Incident Reporting Policy.

Our Team's Responsibilities

- **Medical Director (Dr. Syed Sheik):** Has overall responsibility for data protection compliance, ensuring policies and training are in place, and acting as the main point of contact for data breach escalations.
- **All Staff:** Must comply with data protection rules, only access information they need to do their job (**need-to-know basis**), and report any data breaches or concerns right away.

Data Retention

We only keep your data for as long as we legally need to. When we no longer need it, it will be disposed of securely and confidentially. We follow specific retention schedules based on legal requirements.