Annie Riggs

Registered Homeopath

DATA PROTECTION POLICY

Scope of the policy

This policy applies to the work of homeopath Annie Riggs (hereafter referred to as 'AR'). The policy sets out the requirements that AR has in order to gather personal information for professional purposes. The policy details how personal information will be gathered, stored and managed in line with data protection principles and the General Data Protection Regulation. The policy is reviewed on an ongoing basis to ensure that it is compliant. This policy should be read in tandem with the AR's Privacy Policy.

Why this policy exists

This data protection policy ensures that AR:

- complies with data protection law and follows good practice
- protects the rights of patients
- is open about how she stores and processes patients' data
- protects herself from the risks of a data breach

Data protection principles

The General Data Protection Regulation identifies 8 data protection principles.

Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner

Principle 2 - Personal data can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Principle 3 - The collection of personal data must be adequate, relevant and limited to what is necessary compared to the purpose(s) data is collected for.

Principle 4 – Personal data held should be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

Principle 5 – Personal data which is kept in a form which permits identification of individuals shall not be kept for longer than is necessary.

Principle 6 - Personal data must be processed in accordance with the individuals' rights.

Principle 7 - Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Principle 8 - Personal data cannot be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data.

Certain of these principles are expanded upon in the sections that follow.

Lawful, fair and transparent data processing

AR requests personal information from patients and potential patients for the purpose of consulting with them and providing them with advice and guidance on homeopathic treatments. The forms used to request personal information may contain a privacy statement informing patients and potential patients why the information is being requested and what the information will be used for. Patients should be asked to provide consent for their data to be held and a record of this consent along with patient information will be securely held. Patients will be informed that they can, at any time, remove their consent and will be informed as to what to do should they wish to do so.

Processed for Specified, Explicit and Legitimate Purposes

Patients will be informed how their information will be used and AR will seek to ensure that patients' information is not used inappropriately. Appropriate use of information provided by patients includes:

- Communicating with patients in order to make, change or cancel consultations
- Assessing the conditions and issues reported by patients and devising and prescribing relevant remedies and therapies.

AR will ensure that patients' information is managed in such a way as to not infringe an individual'rights which include:

- The right to be informed
- The right of access
- The right to rectification
- The right to restrict processing
- The right to data portability
- The right to object.

Adequate, Relevant and Limited Data Processing

AR's patients will only be asked to provide information that is relevant to support consultations and prescription. This includes:

- Name
- Date of birth
- Gender
- Postal address
- Email address
- Telephone number
- Medical history
- Personal history

Where additional information may be required, this will be obtained with the specific consent of the patient who will be informed as to why this information is required and the purpose for which it will be used.

There may be occasional instances where a patient's information needs to be shared with a third party due to an accident or incident involving statutory authorities. Where it is in the best interests of the patient or of AR, in these instances where AR has a substantiated concern then consent does not have to be sought from the individual.

Accuracy of Data and Keeping Data up to Date

AR has a responsibility to ensure that patients' information is kept up to date. Patients will be required to let AR know if any of their personal information changes.

Accountability and Governance

AR is responsible for ensuring that her practice remains compliant with data protection requirements and can provide evidence that it has. For this purpose, those from whom data is required will be asked to provide written consent. The evidence of this consent will then be securely held as evidence of compliance.

Secure Processing

AR has a responsibility to ensure that data is both securely held and processed. This includes:

- using strong passwords for information held within computer systems
- restricting access to computer and paper-based files
- using password protection on laptops and PCs that contain or access personal information
- using password protection or secure cloud systems
- providing adequate virus-protection and firewall software to secure computer-based systems.

Subject Access Request

AR's patients are entitled to request access to the information that is held by her. The request needs to be received in the form of a written request to AR.

On receipt of the request, the request will be formally acknowledged and dealt with within 14 days unless there are exceptional circumstances as to why the request cannot be granted. AR will provide a written response detailing all information held on the individual. A record shall be kept of the date of the request and the date of the response.

Data Breach Notification

Were a data breach to occur, action shall be taken to minimise the harm. AR will inform any patients where she believes their personal information has been compromised. Where necessary, the Information Commissioner's Office will be notified.

If a patient contacts AR to say that they feel that there has been a breach by AR, she will ask the patient to provide an outline of their concerns. If the initial contact is by telephone, AR will ask the patient to follow this up with an email or a letter detailing their concern. The concern will then be investigated fully and a response made to the patient. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

Policy review date: May 2020