AUTOIMMUNE CLINIC

DATA PROTECTION POLICY

Contents

1. Introduction

1.1. Purpose of Policy

Autoimmune Clinic needs to gather and use certain information about individuals.

These can include clients, suppliers, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data will be collected, handled and stored to comply with the General Data Protection Regulation.

1.2. Policy Statement

Autoimmune Clinic is committed to a policy of protecting the rights and privacy of clients, staff and others in accordance with General Data Protection Regulation.

Autoimmune Clinic commits to:

- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- register our details with the Information Commissioner's Office (ICO)

1.3. Personal Data

Autoimmune Clinic may hold data for the following purposes:

- Provision of direct healthcare
- Marketing and newsletters
- Case histories

Special categories of data included race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health and sexual orientation.

Autoimmune Clinic may hold special category data for the following purposes:

- Provision of direct healthcare

1.4. Data Protection Principles

There are six data protection principles that are core to the General Data Protection Regulation. Autoimmune Clinic will make every possible effort to comply with these principles at all times in our information-handling practices. The principles are:

1) Lawful, fair and transparent
Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2) Limited for its purpose
Data can only be collected for a specific purpose.

3) Data minimisation
Any data collected must be necessary and not excessive for its purpose.

4) Accurate
The data we hold must be accurate and kept up to date.

5) Retention
We cannot store data longer than necessary.

6) Integrity and confidentiality
The data we hold must be kept safe and secure.

1.5. Key risks

The main risks are in two key areas:

- information about individuals getting into the wrong hands, through poor security or inappropriate disclosure of information
- individuals being harmed through data being inaccurate or insufficient

2. Responsibilities

Autoimmune Clinic is the data controller for all personal data held by us and is responsible for:

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identifying the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Storing data in safe and secure ways
- Assessing the risk that could be posed to individual rights and freedoms should data be compromised

3. Data Recording, Security and Storage

3.1 Data accuracy and relevance

Autoimmune Clinic will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

3.2 Data security

Autoimmune Clinic will keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, we will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

3.3 Storing data securely

- In cases when data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it
- Printed data will be shredded when it is no longer needed
- Data stored on a computer will be protected by strong passwords that are changed regularly. A password manager will be used to create and store passwords.
- Data stored on CDs or memory sticks will be encrypted or password protected and locked away securely when they are not being used
- Cloud services used to store personal data will be assessed for compliance with GDPR principles. An authenticator app will be used to access cloud data.
- Servers containing personal data must be kept in a secure location, away from general office space
- Data will be regularly backed up.
- All servers containing sensitive data must be protected by security software
- All possible technical measures will be put in place to keep data secure

3.4 Data retention

Autoimmune Clinic will retain personal data for no longer than is necessary. This shall be in accordance with the guidelines of our professional association, BANT.

4. Accountability and Transparency

Autoimmune Clinic will ensure accountability and transparency in all our use of personal data. We will keep written up-to-date records of all the data processing activities that we do and ensure that they comply with each of the GDPR principles.

We will regularly review our data processing activities and implement measures to ensure privacy by design including data minimisation, pseudonymisation, transparency and continuously improving security and enhanced privacy procedures.

5. Consent

Autoimmune Clinic will ensure that consents are specific, informed and plain English such that individuals clearly understand why their information will be collected, who it will be shared with, and the possible consequences of them agreeing or refusing the proposed use of the data. Consents will be granular to provide choice as to which data will be collected and for what purpose. We will seek explicit consent wherever possible.

We will maintain an audit trail of consent by documenting details of consent received including who consented, when, how, what, if and when they withdraw consent. For online consent, we may use a cryptographic hash function to support data integrity. Alternatively, we will maintain the consents information in a spreadsheet with links to the consent forms.

We will regularly review consents and seek to refresh them regularly or if anything changes.

6. Direct Marketing

Autoimmune Clinic will comply with both data protection law and Privacy and Electronic Communication Regulations 2003 (PECR) when sending electronic marketing messages. PECR restricts the circumstances in which we can market people and other organisations by phone, text, email or other electronic means.

We will seek explicit consent for direct marketing. We will provide a simple way to opt out of marketing messages and be able to respond to any complaints.

7. Subject Access Requests

7.1 What is a subject access request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

7.2 How to deal with subject access requests

Autoimmune Clinic will provide an individual with a copy of the information requested, free of charge. This will occur within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats (as described in section 4.3).

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual will be informed within one month.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting.

Once a subject access request has been made, we will not change or amend any of the data that has been requested. Doing so is a criminal offence.

7.3 Data portability requests

We will provide the data requested in a structured, commonly used and machine-readable format. This would normally be a PDF file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to within one month.

8. Transferring data internationally

There are restrictions on international transfers of personal data. We will not transfer personal data abroad without express consent.

9. Third Parties

9.1 Using third party controllers and processors

As a data controller and/or data processor, we will have written contracts in place with any third-party data controllers (and/or) data processors that we use. The contract will contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data controller, we will only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

As a data processor, we will only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

9.2 Contracts

Our contracts will comply with the standards set out by the ICO and, where possible, follow standard contractual clauses. Our contracts with data controllers (and/or) data processors will set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

10. Reporting breaches

Any breach of this policy or of data protection laws will be reported as soon as practically possible. This means as soon as we become aware of a breach.

Autoimmune Clinic has a legal obligation to report any data breaches to UK Supervisory authority which is the Information Commissioners Officer within 72 hours.