DATA PROTECTION POLICY

Contents

DATA PROTECTION POLICY

1 Introduction

1.1 Purpose of Policy

David Thunder needs to gather and use certain information about individuals. We need to collect this personal information about your health in order to provide you with the best possible treatment. Your requesting treatment and our agreement to provide that care constitutes a contract. You can, of course, refuse to provide the information, but if you were to do that we would not be able to provide you with our services. It is therefore a condition of any treatment that you give your explicit consent to allow us to document and process your personal medical data. We have a "Legitimate Interest" in collecting your information, because without it we would not be able to do our job effectively and safely.

These details can include medical notes, employer information and referral sources. We will only collect what is relevant and necessary for your treatment.

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

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

David Thunder commits to:

- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- provide training and support to staff who handle personal data, so that they can act confidently and consistently
- Register our details with the Information Commissioner's Office (ICO)

1.3 Personal Data

David Thunder may hold data for the following purposes:

- Provision of Direct Healthcare and relevant communication pertaining to it.
- Marketing and Newsletters (You can opt-out of this at any time.)
- Case Histories
- Staff Administration

Details about your health fall into the a sub-category of personal data known as 'special category data' an example of special category data we hold about you would be your treatment notes.

1.4 Data Protection Principles

There are six data protection principles that are core to the General Data Protection Regulation. David Thunder 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.

1.4.1 Assesments

1.4.1.1 Data Protection Impact Assessment (DPIA)

1.4.1.2 Legitimate Interest Assessment (LIA)

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

David Thunder 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

DATA PROTECTION POLICY

3 Data Recording, Security and Storage

3.1 Data accuracy and relevance

David Thunder will ensure that any personal data we process is accurate, adequate, relevant and not excessive for the purpose that 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

David Thunder 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

- Some of our data is held outside the EEA by our appointed data processors.
- In cases when data is stored on paper it will be kept in a secure place where unauthorised personnel cannot access it and shredded when it is no longer needed.
- Data stored on computer by David Thunder will be protected by strong passwords that are changed regularly, require two-factor authorisation and will be locked away securely when not in use. Data stored on memory sticks or external hard drives 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 using an authenticator app and two-factor authorisation.
- All possible technical measures will be put in place to keep data secure.

3.4 Data retention

David Thunder will retain personal data until you deem our services are no longer required, in order to provide you with the best possible care should you need to see us at a future date. We are legally obligated to store data for a minimum of 7 years or until the age of 25 for minors.

3.5 Website, Forms & Cookies

Some basic personal data may be collected about you from the marketing forms and surveys you complete, from records of our correspondence and phone calls and details of your visits to our website, including but not limited to, personally identifying information like Internet Protocol (IP) addresses.
Our website uses cookies, which is a string of information that a website stores on a visitor's computer, and that the visitor's browser provides to the website each time the visitor returns. Squarespace uses cookies to help us to identify and track visitors and their website access

preferences. Our website visitors who do not wish to have cookies placed on their computers should set their browsers to refuse cookies before using our website, www.dthunder.com.

4 Accountability and Transparency

David Thunder 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 continuously improving security and enhanced privacy procedures.

5 Consent

David Thunder 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.

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

6 Disclosure

We will keep your personal information safe and secure, only staff engaged in providing your treatment will have access to your patient records, although our administration team will have access to your contact details so that they can make appointments and manage your account. We will not disclose your Personal Information unless compelled to, in order to meet legal obligations, regulations or valid governmental requests. The practice may also enforce its Terms and Conditions, including investigating potential violations of its Terms and Conditions to detect, prevent or mitigate fraud or security or technical issues; or to protect against imminent harm to the rights, property or safety of its staff.

7 Direct Marketing

David Thunder 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.

We do not broker your data and you can ask to be removed from our marketing database by contacting us at any time.

8 Data Access Requests

8.1 Your rights as a data subject

At any point whilst we are in possession of, or processing your personal data, all data subjects have the following rights:

- Right of access – you have the right to request a copy of the information that we hold about you.
- Right of rectification – you have a right to correct data that we hold about you that is inaccurate or incomplete.
- Right to be forgotten – in certain circumstances you can ask for the data we hold about you to be erased from our records.
- Right to restriction of processing – where certain conditions apply you have a right to restrict the processing.
- Right of portability – you have the right to have the data we hold about you transferred to another organisation.
- Right to object – you have the right to object to certain types of processing such as direct marketing.
- Right to object to automated processing, including profiling – you also have the right not to be subject to the legal effects of automated processing or profiling.

8.2 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 that should be provided in a privacy notice.

8.3 How to deal with subject access requests

David Thunder 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 7.3).

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.

8.4 To access what personal data is held, identification will be required.

We will accept the following forms of identification (ID) when information on your personal data is requested: a copy of your driving licence, passport, birth certificate and a utility bill not older than three months. A minimum of one piece of photographic ID listed above and a supporting document is required.

8.5 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.

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 that 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.
David Thunder has a legal obligation to report any data breaches to UK Supervisory authority, which is the Information Commissioners Officer within 72 hours.