DR JEREMY CHATAWAY

Context and overview

Key details

- Policy prepared by: Dermott Sales.
- Approved by management on: 20th May 2018.
- Policy became operational on: 24th May 2018.
- Next review date: May 2019

Introduction

Dr Jeremy Chataway needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures Dr Jeremy Chataway:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes

3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

How do we collect information about you?

We keep records about your health and any treatment. These records help to ensure that you receive the best possible care. They may be written down in paper records or held on computer.

We may keep records of medico-legal instruction. These records include not only records on a claimant's health and treatment but also legal documentation relating to the progression of a claim. There records may be written down or held on computer.

It is essential that your details are accurate and up to date. Always check that your personal details are correct when you visit us and please inform us of any changes as soon as possible.

Policy, Risks and Responsibilities

This policy applies to:

- The offices of Dr Jeremy Chataway
- All staff and volunteers of Dr Jeremy Chataway
- All other people working on behalf of Dr Jeremy Chataway

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

Data protection risks

This policy helps to protect Dr Jeremy Chataway and patients from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the practice uses data relating to them.
- **Reputational damage.** For instance, the practice could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Dr Jeremy Chataway has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Data protection officer, Marjan Denis** is responsible for:
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data Dr jeremy Chataway holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

General Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required it must be requested.
- Staff should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the practice or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Staff **should request help** from the data protection officer if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data controller.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Staff should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.

- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or Smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data Usage

Personal data is of no value to Dr Jeremy Chataway unless the he can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by un encrypted email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Staff **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Who we share personal information with

Everyone working within the practice has a legal duty to keep information about you confidential. Similarly, anyone who receives information from us has a legal duty to keep it confidential.

We will not disclose your information to any other third parties except where there is a legitimate interest, we may share information with:

- Medical Professionals engaged by us to carry out services to you.
- Your GP or medical practitioner – we will contact your GP or medical practitioner following an outpatient consultation and with a discharge summary following any inpatient or day case procedure.
- The hospital if you are being treated as an inpatient and require an overnight stay.
- To submit claims relating to your treatment to your insurer or any other third party covering the cost of any treatment or assessment on your behalf.
- The Department of Health or any other statutory body to whom we are required to submit data.
- Authorised organisations to convert your data into an anonymised statistical form.
- We will provide information to progress your medico-legal claim in accordance with your solicitor's instructions and guidance from the Courts.

Data Accuracy

The law requires Dr Jeremy Chataway to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Dr Jeremy Chataway should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- Dr Jeremy Chataway will make it **easy for data subjects to update the information** Dr jeremy Chataway holds about them. For instance, via the company website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Access Requests

All individuals who are the subject of personal data held by Dr Jeremy Chataway are entitled to:

- Ask **what information** the practice holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at [email address]. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged a suitable fee per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Dr Jeremy Chataway will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from any legal advisers where necessary.

Providing and use of Information

Your information may also be used to:

1. Review the care we provide to ensure it is of the highest standard and quality.
2. Ensure our service can meet patient needs in the future
3. Investigate patient queries, complaints and legal claim
4. Prepare statistics on our performance

5. Help train and educate healthcare professionals.
6. As part of the Consultants' regular appraisal based on the GMC guidelines for *Good Medical Practice*

Dr Jeremy Chataway aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

[This is available on request. A version of this statement is also available on the company's website.]