Data Transfer Policy

Last Modified:	July 2023
Reviewed:	
Version:	1

Contents Page

1. Purpose

There are many occasions when information is transferred between departments, to third-party service providers, to other public bodies, commercial organisations and individuals. This is done using a wide variety of media and methods, in electronic and paper format.

In every transfer, there is a risk that the information may be lost, misappropriated or accidentally released. Medical Tracker has a duty of care in handling information.

2. Scope

The scope of this policy covers any type of information (i.e., word documents, PDF reports and excel spreadsheets) in any format and on any medium.

This policy applies to all employees and any third-party that processes any Medical Tracker information.

3. Exclusions

This policy does not cover the transfer of information over the internal network, which has its own automated security controls. It does not cover proprietary secure transfer mechanisms such as BACS financial transfers that have their own separately implemented security requirements.

4. Roles and Responsibilities

Proper definitions of roles and responsibilities are essential to assure compliance with this Policy. In summary these are:

4.1 The sender

The Sender is responsible for ensuring the following requirements of this Policy are met.

- Assessing the information to be sent, in-line with the Risk Assessment section of this policy.
- Ensuring that the identity and authorisation of the recipient has been formally confirmed and documented.
- Obtaining the consent of the Information Asset Owner for the transfer.
- Ensuring that the information is sent and tracked in an appropriate manner.

4.2 Employees

Individual employees are responsible for familiarising themselves with this Policy and ensuring that any information transfer for which they are responsible is done in a compliant manner.

Individual employees must report any suspected or actual security breaches related to data transfer in-line with the Incident Response Policy and the data breach procedure.

4.3 Is it personal information?

Personal information is about a living, identifiable individual. If it contains details of racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, commission of offences, court appearances and sentences it is further classified as sensitive personal information. Anything we do with personal information must comply with the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

Before you make any transfer, you must:

- Ensure that the transfer is legal (in particular under the Data Protection Act & GDPR).
- Ensure that the transfer is necessary (is there a less intrusive way).
- Remove or blackout anything that is not essential for the recipient's purpose.
- Have a documented agreement in place to ensure the recipient understands their responsibilities under the law, particularly what to do with the transfer file after they have extracted the information to their system.

4.4 Is it confidential information?

Confidential information is that which Medical Tracker has a duty of confidentiality. This may include information that affects the business interests of a third party, or for which the sender does not hold copyright e.g., bank details, salary details, contracts, agreements.

Before you transfer you must:

- Ensure that you are not breaching a Non-Disclosure Agreement.
- Ensure that the transfer is necessary (is there a less intrusive way).
- Remove anything that is not essential for the recipient's purpose.
- Have a documented agreement in place to ensure the recipient understands their responsibilities under the law, particularly what to do with the transfer file after they have extracted the information to their system.

5. Risk Assessment

Consider the following before transferring information. If in doubt, please contact the Data Protection Officer (DPO).

Is the transfer legal and necessary?

1. It is dangerous to assume that because someone asks for information that they are necessarily authorised or legally entitled to have it. If you are in doubt, then you should check with DPO.

2. Once you are sure that the transfer is legal and necessary, then you must decide what kind of information you are dealing with. This will determine what security is appropriate.
3. To transfer personal or confidential information without these checks may leave Medical Tracker open to legal and reputational damages and the sender may be subject to disciplinary action.

6. Electronic Mail & Encrypted Links

- All passwords used for logging into Medical Tracker's network, emails and software's must adhere to Password Management Policy
- Any password to open an attached file must be transferred to the recipient using a different method than e-mail.
- E-mail messages must contain clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipient.
- The message and the filename must not reveal the contents of the encrypted file.
- Check with the recipient that their e-mail system will not filter out or quarantine the transferred file.
- The sender must check at an appropriate time that the transfer has been successful and report any issues to their line manager.

6.1 Electronic memory (CD, DVD, Flash media drive)

- Information must be stored encrypted using a product approved by the organisation in accordance with the Encryption policy.
- Any password used must adhere to Password Management Policy.
- Any password or key to open the attached file must be transferred to the recipient using a different method than e-mail, e.g., a telephone call to an agreed telephone number, closed letter.
- Personnel responsible for the removable device must be established.

6.2 Delivery by Post or by Hand

- If the file contains personal or confidential data, first explore alternative measures to transfer information i.e., via email or encrypted links.
- If there are no alternative measures then it is essential that the file, whether electronic or paper is kept secure in transit, tracked during transit, and delivered to the correct individual.
- An appropriate delivery mechanism must be used. The post must be delivered by a secure courier and the delivery must be signed for by the individual.
- The recipient should be informed beforehand that data is being sent so they are aware of when to expect the data.
- Package must be securely and appropriately packed, clearly labelled and have a seal, which must be broken to open the package.
- Package must have a return address and contact details.
- The label must not indicate the nature or value of the contents.
- Package must be received and signed for by addressee only.

6.3 Telephone/Mobile Phone

- Transferred information must be kept to a minimum.
- Personal or Confidential information must not be transferred over the telephone or text messages unless the identity and authorisation of the receiver has been appropriately confirmed.

- Personal or confidential data transfers or downloaded to personal mobile devices are prohibited.

6.4 Lost or Missing Data

Employees should inform their line manager, the DPO, and a director immediately when they become aware that data has been lost or missing.
Medical Tracker will follow the data breach procedure.

6.5 INTERNATIONAL DATA TRANSFERS

Under the GDPR/DPA 20198 sufficient transfer mechanism are required to be in place to permit the transfer of personal data across borders. The transfer mechanisms follow as:

- Adequacy Decision : Transfer to a country on the Europeans Commissions approved list
- Binding Corporate Rules
- Model Clauses (Standard Contractual Clauses)
- Derogations
- Explicit consent

Version history:

Date	Version	Description of changes
July 2023	1.0	