

Dr Khalid Mahmood

MBBS

Section 1 - Overview:

Every day our business will receive, use and store personal information about our customers. It is important that this information is handled lawfully and appropriately in line with the requirements of the [Data Protection Act 2018] and the General Data Protection Regulation (collectively referred to as the 'Data Protection Requirements').

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

Section 2 - Policy:

This policy, and any other documents referred to in it, sets out the basis on which we will process any personal data we collect or process.

This policy does not form part of any employee's contract of employment and may be amended at any time.

The Data Protection Officer is responsible for ensuring compliance with the Data Protection Requirements and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the [Data Protection Compliance Manager/Data Protection Officer] or reported in line with the organisation's Whistleblowing Policy or Grievance Policy.

We are committed to protecting your personal information and to being transparent about what information we hold. The Medical expert understands his obligations to you to help you understand how and why we process your personal data.

Our data protection policy and procedures are governed by the Data Protection Act 1998 and, from 25th May 2018, the EU General Data Protection Regulation (GDPR). The law in this area is changing rapidly and we anticipate this statement may be revised in line with guidance from the Information Commissioner's office.

Section 3 - What is Personal Data:

Personal Data means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).

Section 4 – Processing:

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Section 5 - Sensitive personal data:

This includes personal data about physical or mental health. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

Section 6 - Why we hold your personal data:

We are required to hold your personal data for various legal and practical purposes, without which we would be unable to carry out your instructions. Holding your personal data enables us to meet various administrative and legal obligations.

Section 7 - Lawful basis for processing personal data:

The lawful basis for processing the personal data of Claimants as described in this document is to fulfil a contract with an individual. There is a contractual requirement for you to provide the information detailed. Without this we will be unable to fulfil our obligations which could result in the contract terminating.

Section 8 - Data Protection Principles:

Anyone processing personal data, must ensure that data is:

- Processed fairly, lawfully and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose;
- Adequate, relevant and limited to what is necessary for the intended purposes.
- Accurate, and where necessary, kept up to date;
- Kept in a form which permits identification for no longer than necessary for the intended purposes;
- Processed in line with the individual's rights and 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;
- Not transferred to people or organisations situated in countries without adequate protection and without firstly having advised the individual.

Section 9 - Notifying Individuals

The information we hold about you is primarily information you have provided. We will inform you about:

- The purpose or purposes for which we intend to process that personal data, as well as the legal basis for data processing;

- Where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued;
- The types of third parties, if any, with which we will share or disclose that personal data;
- If the business intends to transfer personal data to a non-EEA country or international organisation and the appropriate and suitable safeguards in place;
- How individuals can limit our use and disclosure of their personal data;
- Information about the period that their information will be stored or the criteria used to determine that period;
- Their right to request from us as the controller access to and rectification or erasure of personal data or restriction of data processing;
- Their right to object to data processing and their right to data portability;
- Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn;
- The right to lodge a complaint with the Information Commissioners Office;
- Other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources;
- Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data;
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual;

If we receive personal data about an individual from other sources, we will provide the individual with this information as soon as possible (in addition to telling them about the categories of personal data concerned) but at the latest within 1 month.

Section 10 - Sensitive personal data held:

The information we hold is that which you provide to us. Records may contain:

- Medical Conditions, medical investigations, medical and other consultations, medication and treatment provided

Section 11 - How your Personal Data is processed:

This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, location data, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others). (I don't

understand this part. I thought all data would come from claimants, their insurers and their medical records)

We will only process personal data for the purposes specifically permitted by the Data Protection Requirements. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

Communications to you may be sent by post, telephone. Your personal mobile phone number will only be used if you have given consent.

If you have concerns or queries about any of these purposes, or how we communicate with you, please contact us & we will always respect a request by you to stop processing your personal data, and in addition your statutory rights are set out below.

Section 12 - Sharing your data with others:

Personal data, including sensitive personal data, may be shared between Parties who legitimately need the information to carry out their normal duties and who we have a contractual obligation or arrangement with. We endeavour to ensure that sensitive personal data is only shared with colleagues or outside companies with your explicit consent.

However, circumstances may arise where this data is shared with colleagues without gaining your consent. This will only occur if it is necessary to protect your vital interests or the vital interests of another person; or for certain other reasons where it is not possible or appropriate to gain your consent such as disclosures to the police for prevention or detection of crime, or to meet statutory obligations relating to equality monitoring.

Otherwise, [DME/Company/medical expert] does not share data with any third party, except as allowed for in other privacy notices or required by law. We do not sell your personal data to third parties under any circumstances or permit third parties to sell on the data we have shared with them.

Section 13 - Transfer of personal data to other countries:

Where data is shared within the UK, or the European Union (EU), the third party will be required to comply with and safeguard the data under the terms of the DPA and appropriate EU regulations. Your personal information will only be transferred to countries, outside of the EU, whose data protection laws have been assessed as adequate by the European Commission, or where adequate safeguards, such as the EU-US Privacy Shield, are in place.

Section 14 - How long data is kept:

We will keep the data only as long as is necessary for the purpose(s) for which it was collected. Data will be securely destroyed when no longer required.

Section 15 - Data Security:

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We have put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We will maintain data security by protecting the confidentiality, integrity, and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on PeopleHR (I don't know what this is) instead of individual PCs.

Section 16 - Security Procedures Include:

- **Clean Desk** – Desks are to remain clean, and no paper documents left unoccupied.
- **Company/medical expert anonymisation and encryption of data.**
- **Methods of disposal** - Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
- **Transferring Personal Data Outside of the EEA**

We may transfer any personal data we hold to a country outside the European Economic Area ('EEA') or to an international organisation, provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms;
- The data subject has given his consent;
- The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject;
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims;

- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Those staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

Section 17 - Your rights:

You have the following rights:

To Be Informed:	This privacy notice provides the information you are entitled to receive:
Access	Please contact us if you would like confirmation that your data is being processed and access to your personal data. There is no charge for us providing you with this data and it will be provided within a month of the request (unless the request is unfounded or excessive).
Rectification	Please inform us of any data which you would like rectified, and we will usually respond within a month of the request. We will pass on the changes to any third parties who need to change their records and let you know this has been done.
Erasure	You may exercise your right to have your personal data erased in a number of circumstances (e.g. if the data is no longer necessary in relation to the purpose for which it was created, or you withdraw your consent). Where possible we will comply with all such requests, though some details are part of the [DME] permanent (permanent what) which cannot reasonably be deleted.
Restrict Processing	You can tell us that we can keep your data but must stop processing it, including preventing future mailings and communications. If possible, we will inform any third parties to whom your data has been disclosed of your requirement.
Data Portability	Your data is across manual records and a database. We will do our best to provide information in a portable format, but it is unlikely that we can create systems to do so.
To Object	If we can, we will stop processing your data if you object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling). We will stop processing your data for direct marketing if you tell us to. (How would there ever be direct marketing?) We will stop processing your data if you object to processing for purposes of research and statistics.
Not to be subject to automated decision-making including profiling	We do not use any automated decision-making

You have the right to lodge a complaint with the Information Commissioner's Office at <https://ico.org.uk/concerns>