**KNIGHTSBRIDGE MEDICAL CENTRE - SARS**

**Individuals Rights**

An individual has the following rights when their personal data is being processed.There is no right of erasure permitted for health records, so this right has been excluded from this document.

1. **The right to be informed.**  
     
   An individual has the right to be informed of the processing of their personal data. This needs to be transparent and should include the purposes for processing their personal data, what data will be processed, your retention periods for that personal data, and who it will be shared with. Contact details of the Data Protection Officer (DPO) and organisations involved should also be included.   
     
   It’s important that the information provided is concise, transparent, intelligible, easily accessible, and it must use clear and plain language.  
     
   It is important that you consider a number of different communication channels.   
    **Checklist**   
   The name and contact details of your organisations involved.  
     
    The contact details of our data protection officer.  
     
    The purposes of the processing.  
     
    The lawful basis for the processing. e.g. consent, legitimate interest.

 The categories of personal data obtained.

 The recipients or categories of recipients of the personal data.

 The retention periods for the personal data.

 The rights available to individuals in respect of the processing.

1. **The right of access.**  
     
   An individual has a right of access, commonly referred to as subject access or data subject access request. This gives an individual the right to obtain a copy of their personal data which can be requested in paper or electronic format.  
      
   If a request is received then you must also confirm the processing and purposes and provide the information that the induvial is entitled to.   
     
     
   **Checklist**   
    Make sure staff can recognise a subject access request by providing awareness training. Remember that in most instances you cannot charge for such requests and a request can be made verbally or in writing.

 Have a procedure and policy in place which is transparent and available to the requestor e.g. posters, website. This procedure and policy should also assist staff in acknowledging the request and making sure that two forms of valid ID are provided such as a passport, birth certificate.

 The procedure should include a set of standard letter templates to acknowledge and process the request. Each request should have its own unique reference number. This request should also be recorded in the individual’s health record.

 Ensuring that the request its appropriately fulfilled so that only information provided is what the person is entitled to.

 Provide the requestor with their information in electronic or paper format within one month unless you can justify an extension which must be explained to the requestor.

1. **The right to rectification.**An individual has a right for information to be changed if it’s not accurate (where a note would be added) or if their personal record is incomplete.   
    **Checklist** Have in place a clear procedure detailing how you would handle and acknowledge such a request and complete within one month.  
     
    Ask for valid ID if you have any doubts about where this request has come from.  
     
    Consider the request and make a note to that record which states clearly if you agree to the change and why. Add to that record a note with those changes.   
     
    If the record is incomplete and you agree the additional personal data should be added to that record, then add to that record and make a note of those changes made.   
      
    If the changes cannot be made for technical or non- technical reasons then a note should be made and added to that clients electronic file.   
     
    You should inform the requestor what actions you have undertaken and justify your decisions. For example, why something hasn’t been rectified.   
     
    You must inform the requestor that they do have a right to go to the Information Commissioners Office. (ICO) if they are dissatisfied with your response.
2. **The right to restrict processing.**This is not an absolute right and only applies in certain circumstances.   
     
   **Checklist** Make sure that you have a procedure in place so that staff can recognise a request for restricting processing which can be made verbally or in writing.

 Ensure that any restriction is recorded and implemented but ensure that you have considered any appropriate exemptions first.   
  
 Respond to the request within one month and inform the requestor. You should also inform the requestor if you intend to re-establish the processing.

1. **The right to data portability.**This rightdoesn’t apply to health records unless it is an explicit consented process/pathway and/or if you are conducting automated decision making.   
    **Checklist** Staff recognise a request for data portability and understand when the right applies through the procedures and policy developed. This should include how a request is acknowledged and registered which can made verbally or in writing. You may ask the requestor for valid ID if required.   
     
    Respond to the request within one month and ensure that any personal data, including pseudonymous data is transmitted securely and, in a format, which is readable to another Data Controller’s IT system. You can extend the time period by a couple of months if the request is complex. In such circumstances you would have to justify the reasoning and inform the requestor.

 You cannot charge for such requests unless the request is manifestly unfounded or excessive. In these circumstances you may charge a ‘reasonable fee’ for the administrative costs.

1. **The right to object.**An individual should be informed of this right through your communication channels e.g. website, posters, and general privacy notice. The individual has an absolute right to stop their data being used for direct marketing, but any other objection needs to be considered.

**Checklist** Staff recognise a request through our procedures and policy. This should include how we acknowledge and register a request which can made verbally or in writing. You cannot charge for such objections unless it manifestly unfounded or excessive.

 Process this request within one month and inform the requestor of your decision and justification if you plan to continue to process their personal data. You should also inform the individual that if they are dissatisfied with your response then they can go to the Information Commissioners Office (ICO).   
  
 It’s important you promote in a transparent way the rights of the individual including the right to object which should be clearly explained in any general privacy notice.

 Consider the objection and record your decision and stop processing if you have no grounds to continue with that processing e.g. it can’t be justified.

 Your decision making must be justified and recorded. For example, you may need to continue to process their data for legitimate purposes including performing a public task.

1. **Rights in relation to automated decision making and profiling.**Automated decision making means a process/pathway whereby the decision is based on automated means (e.g. electronic decision). Profiling means where an organisation is using personal data to evaluate certain things about an individual and incorporates utilising automated means to do this. **Checklist** You must have a lawful basis to carry out profiling and/or automated decision-making and document this in our data protection policy.  
    Detail and explain within any privacy notice how that profile has been created e.g. who has provided the data.

 To protect vulnerable people and children, additional steps must be in place if profiling or automated decision making relates to children or vulnerable people personal data.   
 You must have in place procedures and a policy so that staff are aware of handling any objections to the profiling and automated decision making.

 Only collect the minimum amount of data needed and have a clear retention policy for the profiles we create.

 Make it clear how you can access the data that created your profile.