



DATA PROTECTION & GDPR

PRINCIPLE ONE

CONSENT AND PRIVACY: The GP referring the patient has entered into an agreement with the patient to process their information for healthcare purposes, due to this the patient has 'consented to referral'. But patients still need to be made aware how we use their information once we receive it, which is why we have Privacy Notices, on patient letters, on consent forms, on the website and in the patient waiting room.

PRINCIPLE TWO

DATA PROCESSED ONLY FOR THE 'PURPOSE': Patient data is only processed in order to carry out our service as a healthcare provider. Any additional uses of 'patient identifiable data' needs the express written consent of the patient.

PRINCIPLE THREE

DATA QUANTITY: We will only ever hold the amount of information necessary for us to carry out the service, which would include: patient referral, letter, consent form, report, Images and relevant notes. The only additions to this would be Patient information addendums, safeguarding notices or any written correspondence that would be reasonable to keep if in direct relation to their care.

PRINCIPLE FOUR

DATA QUALITY: We will ensure that all patient information is accurate and relevant to the purpose of the service, we will do this by banding all information – referrals, reports, images etc... together in individual patient files. When adding files, we will make it common practice to check previous patients to see if they have already got a profile by doing a simple NHS number search. Any information that is relevant to their appointment with us or ongoing treatment as a result of an appointment with us will be stored on patient profile and updated with every action. We will routinely ask patients to check their personal identifiable information on their appointment letter or over the phone. When they arrive for their appointment they will be asked to confirm their details when booking in. And prior to their scan, the clinical team will check it against their referral and the patient details on the scanner. If patient data is found to be incorrect at any point of care the staff member receiving the information needs to amend the patient profile and write in the patients notes to state what has been changed and why.

PRINCIPLE FIVE

DATA RETENTION: We will routinely hold patient files as 'active' for 2 years. After 2 years inactivity they will go into long term secure storage and be held for 10 years or up to 25 years for obstetric referrals.

PRINCIPLE SIX

SUBJECT ACCESS REQUESTS: Patients have a right to request information about their healthcare. Patients must make the request in writing and must receive the information as soon as reasonably possible or within one calendar month at the latest. **PATIENT RIGHTS :** Patients have the right to object to processing, have incorrect information rectified and request inaccurate information is deleted.

PRINCIPLE SEVEN

DATA SECURITY Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

PRINCIPLE EIGHT

TRANSFERRING DATA OUTSIDE THE EU: Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Currently non applicable to our service