

Oxford Street Surgery – GDPR Patient information

The General Data Protection Regulation (GDPR) is a new law that determines how your personal data is processed and kept safe, and the legal rights that you have in relation to your own data.

The regulation applies from 25th May 2018, and will apply even after the UK leaves the EU.

What GDPR will mean for patients

The GDPR sets out the key principles about processing personal data, for staff or patients;

- Data must be processed lawfully, fairly and transparently
- It must be collected for specific, explicit and legitimate purposes
- It must be limited to what is necessary for the purposes for which it is processed
- Information must be accurate and kept up to date
- Data must be held securely
- It can only be retained for as long as is necessary for the reasons it was collected

There are also stronger rights for patients regarding the information that practices hold about them. These include;

- Being informed about how their data is used
- Patients to have access to their own data
- Patients can ask to have incorrect information changed
- Restrict how their data is used
- Move their patient data from one health organisation to another
- The right to object to their patient information being processed (in certain circumstances)

What is GDPR

GDPR stands for General Data Protection Regulations and is a new piece of legislation that will supersede the Data Protection Act. It will not only apply to the UK and EU; it covers anywhere in the world in which data about EU citizens is processed.

The GDPR is similar to the Data Protection Act (DPA) 1998 (which the practice already complies with), but strengthens many of the DPA's principles. The main changes are:

- Practices must comply with subject access requests
- Where we need your consent to process data, this consent must be freely given, specific, informed and unambiguous
- There are new, special protections for patient data

The Information Commissioner's Office must be notified within 72 hours of a data breach

- Higher fines for data breaches – up to 20 million pounds

What is 'patient data'?

Patient data is information that relates to a single person, such as his/her diagnosis, name, age, earlier medical history etc.

Oxford Street Surgery – GDPR Patient information

What is consent?

Consent is permission from a patient – an individual's consent is defined as *“any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.”*

The changes in GDPR mean that we must get explicit permission from patients when using their data. This is to protect your right to privacy, and we may ask you to provide consent to do certain things, like contact you or record certain information about you for your clinical records.

Individuals also have the right to withdraw their consent at any time.

Legal and regulatory obligations

To use your information lawfully, we rely on one or more of the following legal bases:

- for the performance of a task carried out in the public interest or it is necessary in the exercise of official authority vested in us
- the performance of a contract
- where the processing is necessary for compliance with our legal obligations
- protecting the vital interests of you or others
- for our organisational legitimate interests; e.g. for incidental and ancillary data processing, for example the management of non-patient or medical databases used for our internal administrative purposes
- where appropriate with your consent
- where necessary for the purposes of preventative or occupational medicine, for the assessment of medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

We also respect the common law duty of confidentiality and to satisfy the common law we may rely on implied consent to share confidential health data for the provision of direct care; for example, when a patient agrees to a referral from one healthcare professional to another.

Health care professionals are required to maintain records about your health including any treatment or care you have received within the NHS (e.g. NHS hospital trust, GP surgery, walk-in clinic, etc.). Using these records helps us to provide the best possible healthcare for our patients.

NHS health records may be processed electronically or on paper or a mixture of both and a combination of working practices and technology are used to ensure that your information is kept confidential and secure.

Records used and stored by this GP practice may include the following information:

- Any contact we have with you, such as appointments, clinic visits, emergency appointments, telephone triage etc.
- Notes and reports about your health
- Details about your treatment and care
- Details about you, including your date of birth, NHS number, address and next of kin etc.
- Results of investigations about you such as laboratory tests, x-rays, etc.

Oxford Street Surgery – GDPR Patient information

- Relevant information from other health professionals, agencies, relatives or those who care for you

This GP practice collects and holds data for the sole purpose of providing healthcare services to our patients and we will ensure that such sensitive information is kept confidential.

However, we may disclose your personal information if:

- (a) It is required by law
- (b) You consent to do so – either implicitly (e.g. for your own treatment and care) or explicitly for other purposes (e.g. sending you newsletters etc.)
- (c) It is justified in the public interest

Some of your personal data will be held centrally and used for statistical purposes. Where we hold data centrally, we take strict measures to ensure that individual patients cannot be identified.

Sometimes information about you may be requested to be used for research purposes. Oxford Street Surgery will always endeavour to gain your consent before releasing such information.

Under the powers of the Health and Social Care Act 2012 (HSCA) the Health and Social Care Information Centre (HSCIC) can request Personal Data from GP Practices without seeking the patient's consent.

Improvements in information technology are also making it possible for us to share data with other healthcare providers with the objective of providing you with better care.

Any patient can choose to withdraw their consent to their data being used in this way. When Oxford Street Surgery is about to participate in any new data-sharing scheme we will make patients aware by displaying prominent notices in the surgery and on our website, providing reasonable notice before the scheme is due to start. We will also explain clearly what you have to do to 'opt-out' of each new scheme.

A patient can object to their personal information being shared with other health care providers, however if this limits the treatment that you can receive then the doctor will explain this to you at the time.

How do we maintain the confidentiality of your records ?

We are committed to protecting your privacy and will only use information collected lawfully in accordance with the GDPR and DPA 18, the Human Rights Act, the Common Law Duty of Confidentiality, the Health and Social Care Act 2012 and the NHS Codes of Confidentiality and Security.

All our staff, contractors and professional members receive appropriate and on-going training to ensure they are aware of their personal responsibilities. They also have employment contractual obligations to uphold your confidentiality, which are enforceable through disciplinary procedures. Your information may be shared internally, including with members of the practice team but only a limited number of authorised staff have access to your personal information (where it is appropriate to their role) and access is only allowed on a strict 'need-to-know' basis.

Oxford Street Surgery – GDPR Patient information

We strive to maintain our duty of confidentiality to you at all times. We will only ever use or pass on personal identifiable information about you if others involved in your care have a genuine need to have it. We will not disclose your information to any third-party without your permission, unless there are exceptional circumstances (i.e. life or death situations), or where the law requires information to be passed on.

We are mindful of the UK information sharing principle following Dame Fiona Caldicott's information sharing review amongst health professionals. We recognise that our duty to share information can be as important as the duty to protect patient confidentiality. Therefore, we encourage our health and social care professionals to have the confidence to share information in the best interests of our patients within the framework set out by the Caldicott principles; 'To share or not to share – the Information Governance Review'.

Who do we share your information with ?

We may also share your information, subject to strict agreements on how it will be used, with other care providers and agencies. These could include:

- NHS and specialist hospitals, trusts
- Other GPs
- Independent contractors such as dentists, opticians, pharmacists
- Private and voluntary sector providers
- GP practice federations
- Ambulance Trusts
- Clinical **Commissioning** groups and NHS England
- NHS Digital
- National Institute for Health and Care Excellence
- Care Quality Commission
- NHS Improvement
- NHS Shared Business Services
- Universities
- Social care services and local authorities
- Education services
- Police and fire and rescue services
- Other 'data processors' during specific project work e.g. Diabetes UK

How do we protect your data ?

We take the security of your data very seriously. We have internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where we engage with third parties to process personal data on our behalf, we stipulate our privacy expectations in written instructions. They are under a strict duty of confidentiality and are

Oxford Street Surgery – GDPR Patient information

obliged to implement appropriate technical and organisational measures to ensure the security of data.

Requesting access to your data

In addition to services such as NHS digital, it has always been possible for a patient to request access to their data at Oxford Street Surgery. The introduction of GDPR legislation makes this legal right clear and ensures that there can be no charge for access to this data.

A request for access to your health records can be made in writing to Oxford Street Surgery using the form at the back of this leaflet. Requests for access can also be made verbally, or in writing, to any member of our staff. You may also email us to make a request and we will facilitate the request through our process.

You should expect that we will require enough proof to satisfy us of your identity. We will aim to verify this as soon as possible after the request has been received. You are not required to give any reasons for the request. A patient can also give written authorisation for a person (for example a solicitor or relative) to make an application on their behalf. We are obliged to carry out sufficient checks to ensure this request is verifiably under the direction of the patient. Children who are able to understand their rights can request data access themselves. In all other cases, a judgement will be made taking into account the best interests of the child and parent/guardian consent. This is by no means an exhaustive list of considerations and individual cases will be dealt with according to their circumstances.

Complaints or Queries

Oxford Street Surgery tries to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures. We are happy to provide any additional information or explanation needed. Any queries you have should be addressed to: the DPO (Data Protection Officer) at:

Sharon Wilson
20 Oxford Street
Workington
CA14 2AJ
01900 604615
Sharon.Wilson@gp-a82050.nhs.uk

Any changes to this notice will be published on our website and on the surgery notice board.

APPLICATION FOR ACCESS TO MEDICAL RECORDS

Subject Access Request

Details of the Record to be Accessed:

Patient Surname	NHS Number
Forename(s)	Address
Date of Birth	

Details of the Person who wishes to access the records, if different to above:

Surname	
Forename(s)	
Address	
Telephone Number	
Relationship to Patient	

Delete as appropriate:

(1) Requests made to access the records of living persons

Declaration: I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health records referred to above under the terms of the Data Protection Act 1998.

(2) Requests made to access the records of deceased persons

Declaration: I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health records referred to above under the terms of the Access to Health Records Act.

Tick whichever of the following statements apply.

- I am the patient.
- I have been asked to act by the patient and attach the patient's written authorisation.
- I am acting in Loco Parentis and the patient is under age sixteen, and is incapable of understanding the request / has consented to me making this request. (*delete as appropriate).

Applicant signature.....Date.....

APPLICATION FOR ACCESS TO MEDICAL RECORDS

Subject Access Request

Details of Application

Patient to complete

(please tick as appropriate)

I am applying for access to view my records only	
I am applying for copies of my medical record	
I have instructed someone else to apply on my behalf	
I have attached the appropriate fee	

Notes:

Under the GDPR and Data Protection Act regulations you do not have to give a reason for applying for access to your health records.

Under the Access to Health Records Act you will/will not need to give reasons for applying for access to a deceased person's health records.

You may be asked to provide photographic identification.

Optional - Please use this space below to inform us of certain periods and parts of your health record you may require, or provide more information as requested above.

This may include specific dates, consultant name and location, and parts of the records you require e.g. written diagnosis and reports. Note: defining the specific records you need may result in lower fee charges and a quicker response.

I would like a copy of all records	
I would like a copy of records between specific dates only (please give date range) below	
I would like copy records relating to a specific condition / specific incident only (please detail below)	