

Privacy Notice for Patients

Who we are

Data Controller	Abbey Road Surgery
Named Data Protection Officer	Ursula Stout, Abbey Road Surgery, Alfred Barrow Health Centre, Duke Street, Barrow in Furness, Cumbria, LA14 2LB

Introduction

We are committed to protecting and respecting your privacy and keeping your information secure.

Personal Data is any information relating to an identifiable person who can be directly or indirectly identified from that data. Identifiers could include name, system ID numbers and location data.

Some forms of Personal Data are considered to be sensitive and must not be processed except for certain limited purposes. These Special Categories of Personal Data include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, details of sex life or sexual orientation and biometric data for the purpose of identifying a natural person.

In order to provide our services, we will collect Personal Data, including Special Categories of Personal Data, about you. We will refer to these collectively as data throughout this notice. We will always treat your data with absolute care to protect your confidentiality.

This notice explains how we collect information about you, how we use that information and who we may share it with. It also tells you about your privacy rights and how the law protects you.

How the law protects you

Data protection laws say that we are only allowed to use the data we hold about you if we have a legitimate reason for doing so, and it is necessary to do so. There are six reasons, or lawful bases, under which we can process data. These are:

- Consent: you have given clear consent for us to process your data for a specific purpose.
- Contract: the processing is necessary for a contract you have with us, or because you asked us to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
- Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's data which overrides those legitimate interests.

A legitimate interest is when we have a business or commercial need to use your information. If we rely on this reason, then we must explain to you what our legitimate interest is. We must consider what is right and best for you when deciding if we want to rely on a legitimate interest.

For Special Categories of Personal Data there are additional safeguards we must meet in order to use this information. Data protection law says that processing of Special Categories of Data is prohibited unless one of ten conditions applies. In order to provide our services we may rely on the following conditions.

- Consent: you have given clear consent for us to process your data for a specific purpose.
- Employment and social security: the processing is necessary to comply with obligations or rights we have in relation to employment and social protection law.
- Vital interests: the processing is necessary to protect someone's life where you are physically or legally unable to give consent.
- Public domain: the information is something that you have already made public.

- Legal: the processing is necessary for the establishments, exercise or defence of legal claims, or if required by a court of law.
- Health and social care: the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
- Public health: the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.
- Archiving: the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Where we collect data and the lawful basis we rely on

We collect and process data about you in order to provide the best quality healthcare to you and to audit the service that we provide. The majority of this data will be obtained directly from you during interactions you have with our services. However, we may also obtain data about you from other sources, as detailed in the section *Data obtained from other sources*. We generally refer to the information we hold about you as your medical record, which is made up of both paper and electronic files.

Data may be obtained from any or all of the following sources.

Our website and social media pages

When someone visits our website or social media page we may collect standard internet log information such as IP address, location and pages visited. We use this data to analyse the effectiveness of our website and visitor behaviour patterns. The information is only processed in a way that does not directly identify anyone. We, and any third party provider we engage to help with the analytics, do not make any attempt to find out the identity of visitors to our website. This privacy notice does not apply to other websites we may provide a link to. We recommend you read the privacy notice on any other websites you visit.

Cookies

Our website uses both persistent and session performance cookies from Google Analytics. A cookie is a small text file placed on your computer or device when you visit a particular website. None of the cookies used on our website collect your personal information and they can't be used to identify you. You can find out more about Google Analytics by visiting the Google Privacy Site at <https://support.google.com/analytics/answer/6004245>. You can opt out of Google Analytics cookies at <http://tools.google.com/dlpage/gaoptout>.

Lawful basis: legitimate interests. These are to enhance and improve the service we offer to our patients and to determine the effectiveness of our informational materials.

Our online services

Online services include the ability to book and cancel appointments, order repeat prescriptions and view your medical record using the internet. The website uses encryption technology to protect your data whilst it is transmitted across the internet.

The online services website is provided and managed by our clinical system supplier, EMIS. For more details of this relationship, see the *Data processors* section below.

Lawful basis: public task.

Special categories conditions: health and social care, public health.

Telephone calls

When someone calls us we collect Calling Line Identification (CLI) information. We use this information to monitor the effectiveness of our business. We may record calls for training and monitoring purposes. Call recording is provided by our telephone service provider. Access to recordings is restricted to specific practice personnel.

Lawful basis: public task.

Special categories conditions: health and social care, public health.

Emails

We may use any email, including any attachments, sent to us to support the services that we provide to you. We may retain details from emails in an anonymised format for monitoring and business development purposes. Emails from patients will be stored in their medical record and may be processed for the purposes of providing relevant services to them.

Our email service is operated by an external provider called Accenture under contract to NHS Digital. For more details of this relationship, see the *Data processors* section below.

Lawful basis: public task.

Special categories conditions: health and social care, public health.

Personal interactions

Personal interactions include visits you make to the practice premises or when a member of the practice team visits you at home. These interactions can be with any member of the practice team, including our reception and admin staff, doctors and nurses.

Data obtained from other sources

Whilst the NHS and local authority work together as one to provide you with the best health and care possible, they are made up of many organisations who are considered as individual Data Controllers under data protection law. We must therefore tell you about data we obtain from other sources.

If you attend another part of the NHS then they will usually share information about the care they provided with us. Examples might be an extended access service, a walk-in centre, an out of hours doctor or a hospital. We may also receive information from your local authority in relation to social care.

We obtain data about you from the following external organisations that provide services local to us.

- University Hospitals Morecambe Bay Trust
- Lancashire and South Cumbria NHS Foundation Trust
- GP Federations, such as Morecambe Bay Primary Care Collaborative
- North West Ambulance Service
- Clinical Commissioning Groups, such as Morecambe Bay Clinical Commissioning Group
- Local Authorities such as South Lakeland District Council
- Social Care Services
- Education Services
- Cumbria Fire and Rescue Services
- Police services such as Cumbria Constabulary
- Voluntary Sector Providers
- Independent Contractors such as dentists, opticians, pharmacists with the practice locality
- Private Sector Providers
- Other 'data processors'

We may additionally receive information from an organisation that is not local if you attend for emergency treatment.

How we share information about you

Your data is treated with strict confidentiality, and we will only ever share information that is relevant and needed for the purpose concerned. The following explains how we share data about you and who this is shared with.

Sharing within the public health and care service (NHS and local authority)

There may be occasions where you need to be seen by another health or care service. Examples include seeing a GP in an extended access service or walk-in centre at a time that suits you, attending an urgent care service or being referred for an investigation or specialist opinion. It is important that these organisations have access to your medical record held by us so they can provide safe and effective care to you as well.

We share data about you with these organisations through paper and electronic means. This may be specific information or your whole medical record depending on the requirements of the service. We only share information in this way to provide you with health and care services.

Lawful basis: public task.

Special categories conditions: health and social care, public health.

Sharing with health professionals outside the NHS

You may have private health insurance and ask us to refer you to a private professional or organisation. This is outside the official functions permitted within our NHS contract which means we will ask for your consent to share information in this way. We would normally share only information that is relevant and not your whole medical record.

Lawful basis: consent.

Special categories conditions: consent.

Sharing not related to health and care provision

We do not share personal data for purposes not related to your health and care provision, except where one of the following applies.

- You have given your explicit and informed consent.
- We believe the sharing is in your vital interests.
- We have a legal obligation to do so.

Anonymised or de-identified data

We may remove all identifiers from data we hold about you to produce pseudonymised or anonymised data sets. These are used for things such as financial claims and service review and design. We refer to use of data in this way as for secondary uses. Once all identifiers have been removed, data is no longer classed as Personal Data as it cannot directly or indirectly identify you. This type of data is not subject to data protection law.

Data processors

We use a number of different systems to hold information. Some of these are internal and under the full control of the practice and some are operated by external providers. Where we use a system from an external provider, they are acting as a Data Processor on our behalf. As a Data Processor, they can only act under our instructions and we have data sharing agreements in place which outline the permissions we grant them.

The data processor is generally providing a system or functionality that we need in order to provide our services to you. There are robust procedures in place that prevent them from viewing the data that we hold within the system they provide. The only exception to this is where we require them to provide us with support, in which case there are protections to limit what they can see.

The following are Data Processors for us.

EMIS

EMIS provide our clinical computer system and online services platform. We hold the majority of your medical record in our clinical computer system. Data is hosted in data centres located in the UK, and within the secure NHS network. Our clinical computer system provides functionality to grant other organisations a view only access to the medical records we hold. This access only works if you are also registered with the other organisation.

Accenture and NHS Digital

The NHS has a secure email system which is procured by NHS Digital through a contract with Accenture. All emails exchanged are encrypted end to end. By default, emails are stored on servers provided by Accenture. Even when downloaded or deleted, a copy of message are stored for a limited period for recovery purposes. The platform is operated using servers and infrastructure based in the UK.

Retention policies

Medical records

We retain all data in line with the Records Management Code of Practice for Health and Social Care 2016. This is available at <https://digital.nhs.uk/media/1158/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016/pdf/Records-management-COP-HSC-2016>.

The standard retention period for GP health records is ten years after the death or emigration of the patient. At this point the records are reviewed to check whether any data needs to be retained for longer. Where it is not known if a patient has died or emigrated and they do not return for any care, the records should be retained for one hundred years.

The retention period for electronic health records depends on the system in use. If the system allows for the record to be deleted whilst retaining a marker to identify it was deleted, then the retention period should be ten years after the patient had died or emigrated. If the system does not allow this, then the record should be archived after ten years so that it is no longer accessible to users of the system.

Your rights

Right to be informed

We are informing you about how we collect and use information about you in this Privacy Notice.

Right of access

We believe in being open and transparent about the personal information we hold about you. You can submit a subject access request under relevant Data Protection legislation to ask if we hold any information about you. If we hold information then we will provide a description of it, explain why we are holding it and can provide a copy if requested to do so. Requests must be made in writing and should be sent to the Data Controller at our registered office address. We must provide a response, or the data we hold, within one month of receiving your request.

Right of rectification

If you believe the data that we hold is inaccurate or incomplete then you can ask us to update it. You can do this verbally or in writing, and we must respond to let you know our decision within one calendar month. If we agree the data is inaccurate we will update it, otherwise we will explain why we believe the data we hold is accurate. This right applies to factual information. The opinion of a healthcare professional would not normally be considered factual information and may not be covered by this right.

Right to erasure (right to be forgotten)

In certain circumstances you can ask us to delete all data we hold about you. You can make such a request verbally or in writing and we must respond within one month. The right to erasure does not apply where we have relied on the public task lawful basis for processing. If we need to retain the data in order to defend against any legal claims, we may not be able to comply with your request.

Right to restrict processing

In certain circumstances you can ask us to stop processing any the data we hold about you. We can still retain the data, but we cannot use it. Such requests can be made verbally or in writing and we have one month to respond. You can ask us to stop processing data if:

- you believe the data is inaccurate;
- the data has been unlawfully processed;
- you disagree with our legitimate interests for processing your data.

We will stop processing data on receipt of your request. This restriction may be removed once we have provided our response.

Right to object

Where we process data for our legitimate interests, direct marketing, public task or public interest, you have a right to object to this processing. Any objection must be on grounds relating to your particular situation. If you object to our legitimate interests then we must be able to demonstrate that our interests override your own interests, right and freedoms. We cannot refuse your right to object to direct marketing.

If you have provided us with consent, you have a right to withdraw this consent at any time. You will be provided with information about this right when you are asked for consent.

Information about automated processing

We do not carry out any automated processing on the data we hold about you. There is human intervention in all decisions about your care.

If you would like to discuss any of your rights with us then please contact us using the details provided above.

Consequences of not providing your data

We rely on the public task lawful basis as we have a contractual requirement to record details of the healthcare that we provide to you. This ensures we have all relevant information to provide you with the best possible care and treatment. If you did not provide us with information, then it may limit our ability to provide you with safe care and treatment as we may be unable to determine the clinical risk involved.

How to withdraw your consent

Where you have provided consent to us processing your data, you can withdraw this consent at any time. Please contact us if you want to do so.

If you withdraw your consent, we may not be able to provide certain products or services to you. If this is the case, we will tell you.

How to complain (including to ICO)

If you are unhappy with how we have handled your data, then please get in touch with us to discuss your concerns. You can get in touch using any of the contact details provided above.

You can also complain to the Information Commissioner's Office if you are concerned about how we have handled data we hold about you. Full details of how to do so can be found on their website at <https://ico.org.uk/concerns/>. If you prefer you can call them on 0303 123 1113 or email casework@ico.org.uk