

Privacy Notice

Overview of Information Held and Shared

This Privacy Notice explains and describes how Seafield Medical uses and manages the information it holds about its patients. This includes how the information may be shared with other organisations, and how the confidentiality of information is maintained.

Our Contact Details

Organisation Name	Seafield Medical
Address	207 Seafield Road, Bournemouth, BH6 5LL
Phone number	01202 900609
Email	info@seafieldmedical.com
Data Protection Lead	Rosie Green
Information Commissioner's Office Ref	ZB209708

What type of information do we hold about our patients?

We collect and process the following information about our patients:

- identity details – name, date of birth;
- contact details – address, telephone, email address;
- 'Next of Kin' details – the contact details of a close relative or friend;
- details of any carer you may have, or anyone you care for;
- details of any appointments with the GP;
- reports from secondary care of any A&E visits, inpatient stays or clinic appointments;
- results of any scans, X-rays and pathology tests requested;
- details of any diagnosis and treatments given;
- details of any longstanding health concerns and conditions;
- details about your health, treatment and care and other relevant information from health professionals, care providers or relatives who care for you;
- information about any allergies;
- information about any DNAR decisions and any living wills that we know of;
- correspondence from other Health and Social Care providers that provide you with services.

Sharing patient information

As an independent medical practice, we do not routinely share your personal information with the NHS or any other third parties. There are occasions where sharing information is important in providing safe medical care or may be beneficial to you, but we will ensure we have your consent beforehand. If you do consent to this, your information will be shared securely. This would include doctors, nurses and allied health professionals, but may also include administrative staff who deal with booking appointments or typing clinic letters.

Access to information is strictly controlled and restricted to those who need it in order to do their jobs. All of our staff receive annual mandatory training on confidentiality and data security and are obliged to respect data protection and confidentiality.

Who we share with

Seafield Medical shares and receives patient information from a range of organisations or individuals for a variety of lawful purposes, including:

- disclosure to hospitals and other NHS staff for the purposes of providing direct care and treatment to the patient, including administration;
- disclosure to social workers or to other non-NHS staff involved in providing health and social care;
- disclosure to staff for the purposes of clinical auditing;
- disclosure to those with parental responsibility for patients, including guardians;
- disclosure to carers without parental responsibility;
- disclosure to the manager for the purpose of planning, managing and auditing healthcare services;
- disclosure to bodies with statutory investigative powers e.g. the Care Quality Commission, the GMC, the Audit Commission and Health Services Ombudsman;
- fire and rescue services – emergency;
- ambulance trusts;
- voluntary sector providers;
- independent contractors such as dentists, opticians, pharmacists;
- disclosure to solicitors, insurance companies, the police, the Courts (including a Coroners Court) and to tribunals and enquiries.

Confidential patient identifiable information is only shared with other organisations where there is a legal basis to do so, such as:

- when the patient has given his/her explicit consent to the sharing;
- when there is a Court Order to share patient data;
- when the patient has implicitly consented for the purpose of direct care;

Patient identifiable information is only shared on a need to know basis, where there is a direct purpose to do so, limited to what is necessary for that purpose. Patient information may be shared, for the purposes of providing direct patient care, with other NHS provider organisations such as NHS Acute Trusts (hospitals), NHS Community Health, other NHS General Practitioners (GPs), NHS Ambulance services in order to maintain patient safety; this data will always be identifiable.

For the benefit of the patient, Seafield Medical may also share information with non-NHS organisations which are also providing healthcare. These non-NHS organisations may include, but are not restricted to: social services, education services, local authorities, the police, voluntary sector providers, and private sector providers.

Patients are not legally or contractually obliged to share information with their healthcare provider, however, your care will be affected if your clinicians do not have the relevant information necessary in order to diagnose and treat you.

Purposes of Processing

Seafield Medical processes patient data for the following primary purposes:

- providing direct health care;
- providing other healthcare providers with information regarding your healthcare;
- supporting social care with safeguarding vulnerable patients.

We keep records in order to:

- have accurate and up to date information available to the right care and treatment options;
- have information available to clinicians that you may see or be referred to at NHS organisations or organisation providing healthcare services.

Clinical System - Electronic Patient Records

Seafield Medical uses an electronic patient record to securely process and share information between our staff. This means that the doctor who is caring for you can see your medical history, including any allergies and current medications, to provide you with safe care.

Seafield Medical uses Heydoc integrated Clinical System as our Electronic Patient Record. You can find out more about Heydoc on their website here: heydoc.co.uk

Our Website

Our website will ask for your consent to use cookies to track your activity online for marketing purposes.

Other Ways in Which Patient Information May Be Used:

Incident management

If you are involved in an incident, for example you slip and fall whilst in the doctor is visiting you, your information may be included in the incident report and used as part of the investigation process.

Complaints and Queries

If you raise a complaint or query with Seafield Medical, information will be held about you within the secure cloud-based file storage in order to ensure that your complaint or query is answered appropriately. Details of complaints or queries will not be stored within your medical records.

Invoice Validation

Invoice validation is an important process to ensure our financial records are accurate and up to date.

Improving Services

Data may be used for audit purposes and for planning, managing and improving our service.

Data controller and processors

Seafield Medical is the Data Controller of the data which we gather, hold and create about you.

The Practice engages with data processors who may process your data. All Data Processors are held to strict contractual obligations, which specify the limitations, any access arrangements, storage and retention of data on our behalf as well as strict confidentiality and information handling clauses. All data processors are also held to high information security standards and asked to provide evidence of how they meet Data Protection legislation. An example of these processors would be software suppliers.

Retention Periods

The Practice works to the Records Management Code of Practice for Health and Social Care 2016 Retention Schedule. <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016>

Data Subject Rights

The law gives you certain rights to your personal healthcare information that we hold:

1. Right of access to your information

You have the right to request a copy of the personal information that we hold about you; this is known as a Subject Access Request. We have one month to reply to you and give you the information that you require. This can be extended by two further months if the request is complex or we have received a number of requests from you. Subject Access Requests can be made by you the patient, by a legal representative; a solicitor acting on your behalf, a carer, parent, guardian or appointment representative, with appropriate consent. A personal representative also has the right of access to deceased records.

If you would like a copy of the information we hold about you, please contact Rosie Green using the contact details on page 1.

We will provide this information free of charge however, we may in some limited and exceptional circumstances have to make an administrative charge for any extra copies if the information requested is excessive, complex or repetitive.

We can restrict disclosure of your information if your doctor feels that granting access would disclose information likely to cause serious harm to your physical or mental health or that of another individual, and where you do not already know the information. Or where granting access would disclose information relating to or provided by a third party who could be identified from the information, and who has not provided consent for it to be released.

2. Right to restrict or object to the use of your information

We cannot share your information with anyone else without your consent.

The right to restrict processing of healthcare data can only be exercised in the following circumstances:

- the accuracy of the data is contested;
- the processing is unlawful.

3. Right to have incorrect information corrected

If you feel that information held about you is incorrect, you have the right to ask for it to be corrected. This applies to matters of fact, not opinion. Incorrect contact information such as your address will be corrected immediately. If the information is of a clinical nature, this will need to be reviewed and investigated by Seafield Medical, which will result in one of the following outcomes:

- Seafield Medical considers the information to be correct at the time of recording and will not amend the data. A statement from you may be placed within the record to demonstrate that you disagree with the information held. You have the right to appeal to the Information Commissioner;
- Seafield Medical agrees that the information is incorrect, however it is not legal to modify or remove information within the record as it represents 'historical information' which may have influenced subsequent events or decisions made. In these circumstances, a note will be made in the record which advises the reader of the inaccuracy and of the correct facts. Seafield Medical will agree the content of the note with you.

4. Right to data portability

This right only applies where the original processing is based on the data subject's consent or fulfilment of a contract that they are party to, and if the processing is automated. However, in the spirit of the Regulations, you have the right to request that your personal and/or healthcare information is transferred, in an electronic or other form, to another organisation.

5. Right to appropriate decision making

The right to appropriate decision making applies to automated processing, including profiling, which produces legal outcomes, or that significantly affects you. Seafield Medical has not identified any automated processing which is solely automated and without human involvement in the outcome of the processing.

6. Right to erasure

This is sometimes known as the right to be forgotten, but it is not an absolute right. You cannot ask for this right of erasure in relation to records which Seafield Medical is legally bound to retain. Seafield Medical

has an obligation, not only to retain information for a specified time period, but also not to retain information for longer than is necessary and will dispose of information securely.

Please see above section on retention.

7. Right to lodge a complaint

If you are dissatisfied with the handling of your personal information, you have the right to make a complaint. In the first instance, formal complaints should be addressed to Rosie Green using the contact details on page 1.

You also have the right to make a complaint to the Information Commissioner's Office – the independent regulator of data protection:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

You can also use their online submission: <https://ico.org.uk/global/contact-us/>

The Law Explained

Data Protection Principles

There are six core principles to data protection legislation:

1. Personal data must be processed lawfully, fairly and transparently (lawfulness, fairness and transparency).
2. Personal data must be collected for specific, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes (purpose limitation).
3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
4. Personal data must be accurate and up to date (accuracy).
5. Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation).
6. Personal data is processed in a manner that ensures appropriate Security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

Lawful basis

The Practice processes personal data for **primary purposes** under the following legal bases:

SEAFIELD MEDICAL

- **General Data Protection Regulations 2016/679 Article 9(2)(h):**

"Processing is necessary for the purposes of preventative 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 and social care systems and services on the basis of Union or Member State law or pursuant to contact with a health professional and subject to the conditions and safeguards referred to in paragraph 3"

Paragraph 3: *"Personal data referred to in paragraph 1 [special categories of data] may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of a professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies."*

Seafield Medical processes special categories of data for secondary purposes under the following legal basis:

- **General Data Protection Regulations 2016/679 Article 9(2)(i):**

"Processing is necessary for reasons of public interest in the areas 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, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy."

Occasionally, the Practice may rely on consent as a legal basis:

- **General Data Protection Regulations 2016/679 Article 6(1)(a):**

"the data subject has given consent to the processing of his or her personal data for one or more specific circumstances"

- **General Data Protection Regulations 2016/679 Recital 43** specifies that for consent to be freely given it

"should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."

Seafield Medical upholds transparency and fairness through the use of this privacy notice. We uphold data minimisation techniques like pseudonymisation and anonymisation where possible to protect data and ensure that the purpose of processing is relevant and adequate.

Seafield Medical holds data security in the highest importance; our systems have role based access and clinical systems are auditable to ensure transparency in the use of systems by staff. Devices are encrypted and all our staff undertake annual mandatory data security training.