Organisation Name: The Birches Medical Centre

Privacy Notice – Practice

Version	Edited by	Date issued	Next review date
1.0	**Liz Heimes Practice Manager**	**07/09/2026**	**07/09/2027**

Position	Named individual
Practice Manager	Liz Heimes
Data Protection Officer (DPO)	gmhscp.icpdpo@nhs.net
Data Controller	Liz Heimes

Overview for all staff

- This privacy notice details the requirement for this organisation to commit to protecting the privacy and confidentiality of all whose information it processes and how it will comply.

- This organisation will ensure that any personal data is processed in accordance with Article 5 of the UK GDPR and information about how this is done will be provided to applicants in a format that is compliant with Article 12 of the UK GDPR.

- Most requests for medical information are made via a Subject Access Request and are usually from a patient or their representative, such as a solicitor or via a Lasting Power of Attorney.

- All clinical records are retained in accordance with NHS England's Records Management Code of Practice with retention periods being dependent on the type of record.

- This organisation has a legal and professional responsibility to safeguard children and adults at risk. Confidential information may therefore be shared without consent to protect any individual or others from serious harm.

- Should a data breach be suspected, then all staff must report this as soon as practicable and within 24 hours of the incident being identified.

Table of contents

1 Introduction

1.1 Policy statement

This policy outlines how this organisation will provide information to patients regarding how patient data is processed for the provision of direct care, research, audit and screening programmes and specific patient groups.

This privacy notice details the requirement for this organisation to commit to protecting the privacy and confidentiality of all whose information it processes and how it will comply. The relevant legislation and regulations to support compliance are detailed at Annex A, whereas a Privacy Notice detailing information for patients about how this organisation supports their data is detailed at Annex B.

This policy is to be read in conjunction with the organisation's Confidentiality and Data Protection Handbook, Confidentiality and Caldicott Policy and also the UK General Data Protection Regulation (UK GDPR) Policy.

UK General Data Protection Regulation (UK GDPR) eLearning is available in the HUB.

1.2 Status

In accordance with the Equality Act 2010, we have considered how provisions within this policy might impact on different groups and individuals. This document and any procedures contained within it are non-contractual, which means they may be modified or withdrawn at any time. They apply to all employees and contractors working for the organisation.

2 Compliance with regulations

2.1 Legislation and regulation

As general practices are expected to collect, store, use, protect and share personal information about patients, and when relevant, staff members, visitors, family, carers, representatives and any others who may interact with their organisation, there is a requirement to strictly adhere to the relevant UK data protection and confidentiality laws.

There is also a requirement to comply with the relevant NHS and regulatory requirements. These are detailed and linked throughout this document, and also listed at Annex A.

2.2 Processing data

This organisation will ensure that any personal data is processed in accordance with Article 5 of the UK GDPR and information about how this is done will be provided to applicants in a format that is compliant with Article 12 of the UK GDPR.

2.3 Communicating privacy information

This organisation must provide information to applicants about how their data is processed in the form of a Practice Privacy Notice.

The Information Commissioner's Office has provided guidance titled Checklists that can be used to support the writing of this privacy notice. Note the template aligns with the NHS England guidance titled Privacy Notice (PN).

2.4 Subject access requests

Most requests for medical information are made via a Subject Access Request (SAR) and are usually from a patient or their representative, such as a solicitor or via a Lasting Power of Attorney.

Following a SAR, should it be deemed that an entry is clinically or factually inaccurate, an appropriate correction will be considered. Should a patient disagree with the content, the organisation will not normally delete a clinical record simply because of their challenge. In these instances and when appropriate, an explanatory statement may be added to the record.

Guidance can be sought from:

- NHS England's Amending patient and service user records
- MPS guidance titled When a patient wants to amend their medical records

The organisation's Access to Medical Records and Online Services Policy includes additional information and also a SAR application form template.

2.5 Retention of clinical records

All clinical records are retained in accordance with NHS England's Records Management Code of Practice with retention periods being dependent on the type of record.

2.6 Use of artificial intelligence

Artificial Intelligence (AI) use is the biggest and fastest moving change to computing in recent years and is becoming commonplace across all industries including primary care. With this being new technology, there is a requirement for additional governance measures to ensure its use is safe and does not expose personal data about both patients and staff to any unnecessary risks.

Examples of AI use include:

- Generation of business meeting notes and any action points
- Support for clinicians during consultations to compile and document medical records
- Generation of summaries of various team meetings when service users and patient cases are discussed

Prior to introducing AI tools and in support of the Data Protection Impact Assessment (DPIA), this organisation will assess the following:

- Purpose
- Necessity
- Proportionality
- Lawful basis
- Confidentiality
- Security
- Supplier arrangements
- Data location
- Retention
- Access
- Transparency
- Risks

For further information, including how this organisation will comply with the Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025, refer to the organisation's Privacy Notice – Artificial Intelligence and the Artificial Intelligence (AI) Usage Policy.

For a DPIA template, refer to the organisation's UK GDPR Policy.

2.7 Statutory disclosures when consent is not required

There are circumstances when this organisation may be required or permitted to disclose information without obtaining the consent of a person and this includes:

- Safeguarding
- Preventing or detecting serious crime
- Public health requirements
- Notification of certain infectious diseases
- Statutory reporting
- Court orders and/or legal obligations
- Requests from regulatory authorities
- Investigations by authorised bodies
- Coroners' investigations
- Fraud prevention
- When disclosure is necessary to protect someone from serious harm
- When disclosure is otherwise authorised by law

The National Health Service Act 2026 at Section 251 together with the Health Service (Control of Patient Information) Regulations 2002 provide statutory mechanisms in certain circumstances for confidential patient information to be used without consent.

It should be noted that this organisation will only disclose information that is relevant and proportionate to the circumstances.

2.8 Safeguarding

This organisation has a legal and professional responsibility to safeguard children and adults at risk. Confidential information may therefore be shared without consent as necessary and as proportionate in order to protect an individual or others from serious harm.

2.9 Children and young people

Children have rights concerning their personal information. At this organisation, we will always consider:

- The child's age
- Maturity
- Their understanding
- Capacity
- Confidentiality
- Parental responsibility
- The child's best interests
- Safeguarding considerations

When a young person is considered competent to make decisions about their healthcare, confidentiality will normally be respected. A parent or person with parental responsibility does not automatically have an unrestricted right to access a child's medical information and as detailed within the organisation's Consent Guidance.

Further reading can be found in NHS England's guidance titled Children and young people, CQC GP mythbuster 8: Gillick competency and Fraser guidelines and also the organisation's Privacy Notice – Easy Read.

2.10 People who lack capacity

When a person is considered to lack capacity to make a particular decision, information will be handled in accordance with the organisation's Mental Capacity Act Policy and Safeguarding Handbook to ensure the best interests of the patient are always considered.

Further reading can be found in the NHS guidance titled Mental capacity.

2.11 Deceased patients

Whilst confidentiality continues after death, the Data Protection Act 2018 and subsequently the UK GDPR only refers to living individuals. As such, for deceased persons, access to their information is a request under the Access to Health Records Act 1990 (AHRA).

Further reading can be found in the organisation's Access to Deceased Patients' Records Policy.

2.12 Opting out

Should a patient not wish for their information to be shared outside of this organisation, then they can request to opt-out of data sharing. There are two different types of opting out:

Type	Description	Actions
Type 1 Opt-out	This is to stop identifiable or confidential information held in a patient's GP record being disclosed outside this organisation for purposes other than their individual care. NHS guidance titled Opt out of sharing your health records	The patient informs the organisation and this is locally coded to their clinical record.
National Data Opt-out **(NDO-O)**	This is to stop confidential patient information being used for research and planning purposes by NHS and other healthcare organisations. Refer to the following NHS guidance: • Make your choice about sharing data from your health records • National Data Opt-Out	Contact NHS England to opt-out. This action cannot be completed by the organisation

	• Setting or changing a national data opt-out choice	

Further reading on the NDO-O is available for patients within Annex B and for staff below and at Annex C:

- National Data Guardian for Health and Care – review of data security, consent and opt-outs
- National data opt-out – data protection impact assessment
- National data opt-out training
- Guidance for health and care staff
- Supporting your patients – information and resources
- Information for GP practices

2.13 General practice data for planning and research collection

NHS England advises that the General Practice Data for Planning and Research (GPDPR) programme has been designed to help the NHS to:

- Monitor the long-term safety and effectiveness of care
- Plan how to deliver better health and care services
- Prevent the spread of infectious diseases
- Identify new treatments and medicines through health research

NHS England's About the GPDPR programme and Looking after your data provide additional information on data sharing. Information for staff should they be asked about opting out can be found at Annex C.

2.14 Data breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Should a data breach be suspected, then all staff must report this as soon as practicable and within 24 hours of the incident being identified.

Further reading can be sought from the organisation's Information Governance Breach Reporting Policy.

2.15 Data complaints

Should a complaint be received then the organisation's Complaints Procedure is to be followed.

Specifically, for a data complaint, in addition to being able to complain to the practice, or ICB, the complainant may also direct their complaint to the Information Commissioner's Office (ICO) should they be dissatisfied with the initial response from the organisation. This is detailed within its guidance titled How to deal with data protection complaints. As for any other complaint, a patient may also escalate their complaint to the Parliamentary and Health Service Ombudsman (PHSO).

Further reading to support the changes following the implementation of the Data (Use and Access) Act 2025 can be found in:

- NHS England document titled Personal data breaches and related incidents
- ICO guidance titled How to make a data protection complaint to an organisation

2.16 Privacy notice review

This privacy notice will be updated:

- At least annually
- Should there be a significant change in legislation
- When NHS England or Department of Health and Social Care (DHSC) issue significant new information governance guidance
- Should ICO guidance materially change
- If the Care Quality Commission's requirements change
- Should this organisation introduce significant new systems or processing activities
- Following a review, or investigation into a significant data protection incident when the notice needs amendment

As for all updates of policies and procedures, this organisation will maintain the version history of all previous privacy notice documents.

Annex A – Legislation and regulations

In addition to the various supporting links throughout this document, the following are deemed as the key sources to this privacy notice and the organisation's supporting information governance framework

Relevant legislation:

- Data Protection Act 2018 (incorporating UK GDPR at Part 2, Chapter 2)
- Data (Use and Access) Act 2025
- Privacy and Electronic Communications Regulations 2003 (PECR)
- Health and Social Care Act 2008 and the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 including Regulation 10 and Regulation 17
- National Health Service Act 2006, including Section 251
- Health and Social Care Act 2012
- Health Service (Control of Patient Information) Regulations 2002
- Access to Health Records Act 1990
- Mental Capacity Act 2005
- Mental Health Act 1983
- Children Act 1989 and 2004
- Care Act 2014
- Human Rights Act 1998
- Equality Act 2010

Regulation and guidance

NHS England	• The common law duty of confidentiality and consent • Data protection policy • Confidentiality policy • Information governance and data protection • Data and Clinical Record Sharing • Keeping GP Records • Records Management Code of Practice
National Data Guardian	• The Eight Caldicott Principles • Review of Data Security, Consent and Opt-Outs
Care Quality Commission	• Regulation 10: Dignity and Respect • Regulation 17: Good Governance
Information Commissioner's Office	• Right to be informed

Annex B – Practice privacy notice

Introduction

At The Birches Medical Centre all staff have a legal responsibility to maintain the confidentiality of those who use our services. Further to this, annual training is undertaken to support the need to maintain confidentiality, data security and information governance. Staff confidentiality obligations continue after their employment, or after their engagement with the practice ends.

Another of our legal responsibilities is to explain how we use any personal information we collect about you at the organisation. This information is in both electronic and paper format.

Why do we have to provide this privacy notice?

We are required to provide you with this privacy notice by law. It provides information about how we use the personal and healthcare information we collect, store and hold about you. If you have any questions about this privacy notice or are unclear about how we process or use your personal information or have any other issue regarding your personal and healthcare information, then please contact our Data Protection Officer Shavarnah.purves@nhs.net

The main things the law says we must tell you about what we do with your personal data are:

- We must let you know why we collect personal and healthcare information about you
- We must let you know how we use any personal and/or healthcare information we hold about you
- We need to inform you in respect of what we do with it
- We need to tell you about who we share it with or pass it on to and why
- We need to let you know how long we can keep it for

The General Data Protection Regulation (GDPR) became law on 24 May 2016. This was a single EU-wide regulation on the protection of confidential and sensitive information. It entered into force in the UK on the 25 May 2018, repealing the Data Protection Act 1998.

Following Brexit, the GDPR became incorporated into the Data Protection Act 2018 (DPA18) at Part 2, Chapter 2 titled The UK GDPR.

What data will be collected by this organisation?

The following data will be collected:

- Patient details (name, preferred name, gender, date of birth, NHS number)
- Address, including previous addresses, emergency contact and NOK information
- Contact details including telephone, email and contact preferences
- Language and accessibility requirements
- Information about carers or representatives
- Medical notes (paper and electronic)
- Treatment and care, including medications, results including pathology, X-ray etc.
- Administrative information including appointment information, registration details, details of any complaints and compliments, any access needs
- Any other pertinent information

The UK GDPR gives extra protection to more sensitive information known as 'special category data'. Information concerning health and care falls into this category and has to be treated with greater care. Data that relates to criminal offences is also considered particularly sensitive.

We collect and use the following more sensitive information (including special category data) that includes data about your:

- Physical or mental health (for example, details about your appointments or diagnosis)
- Racial or ethnic origin
- Sex life
- Sexual orientation
- Genetic data (for example, details about a DNA sample taken from you as part of a genetic clinical service)
- Biometric data (where used for identification purposes), for example fingerprints or facial recognition
- Religious or philosophical beliefs
- Political opinions
- Trade union membership
- Criminal or suspected criminal offences

Where does the data come from?

This organisation may obtain information from the following sources:

- Directly from you, including information provided to this organisation following an online request
- From parents, guardians or representatives when appropriate
- Other healthcare professionals
- NHS England, hospitals, NHS Trusts, community services and pharmacies
- Social care, mental health and ambulance services
- NHS screening programmes, national NHS systems and public health organisations
- Local authorities including safeguarding organisations
- Other organisations involved in patient care
- When legally permitted, from other third parties.

This organisation will only collect information that is relevant and necessary for the purposes for which it is processed.

Using your information

This organisation may share information with the following types of organisations:

- Organisations that provide health and care services (such as hospitals, councils, care homes, and GP surgeries)
- IT and other systems suppliers
- Planners of health and care services (such as Integrated Care Boards, NHS England, and the Department of Health and Social Care)
- Other organisations including the police and government organisations

We will use your information so that we can:

- Assess your health
- Diagnose illness
- Provide treatment
- Prescribe medication
- Arrange referrals
- Receive and review your test results
- Coordinate care

- Communicate with other healthcare professionals
- Support continuity of care (such as information for out of hours and emergency care)
- Provide preventative healthcare, such as for screening and vaccination services
- Manage long-term conditions including end-of-life care
- Check and review the quality of care we provide

.

What is our lawful basis for using information?

Under the UK GDPR, we must have a "lawful basis" for collecting and using your personal information. The lawful basis we rely on for using personal information is:

Lawful basis	Detail
We have your consent. This means you have agreed that we can use or share your personal information	This must be freely given, specific, informed and unambiguous. It is not appropriate to rely on consent for individual care, research or service planning, even if you have obtained consent for other reasons. It is appropriate to rely on consent for the use of some types of cookies on websites.
The law requires us to do this	For example, when NHS England or the courts use their powers to require the data. See this list for the most likely laws that apply when using and sharing information in health and care.
We need it to perform a public task	A public body, such as an NHS organisation or a social care organisation run by a local authority, is required to undertake particular activities. This is mostly likely to be relevant for these organisation's provision of NHS and social care services regulated by the Care Quality Commission. See this list for the most likely laws that apply when using and sharing information in health and care.

We have a recognised legitimate interest. This means that we have a good reason, and that the law has decided that this reason is in the public interest	This cannot be relied on by public authorities in the performance of their tasks. However, it is likely to apply in many circumstances for private providers in health and care. The Data (Use and Access) Act 2025 introduced these recognised legitimate interests as cases when a legitimate interest assessment is not required. If you have selected this lawful basis, confirm below which option applies.

Your rights under the data protection law

Subject to legal exemptions and the circumstances of the processing, you may have the following rights. For full guidance refer to the Information Commissioner's Office guidance titled A guide to individual rights.

Should you wish to access information about you, then a request can be made via a 'Subject Access Request'. For further information discuss this with a member of the team. Please note that the organisation will have to verify your identity before releasing any information and it should also be noted that there may be circumstances when information may be withheld because of a legal exemption.

Instances when information can be disclosed without consent

There are circumstances when this organisation may be required or permitted to disclose information without obtaining your consent as this may be a need under a statutory notification.

Categories include the following:

- Safeguarding
- Preventing or detecting serious crime
- Public health requirements
- Registering a birth or death
- Notification of certain infectious diseases
- Statutory reporting
- When a public inquiry requires the information
- Court orders and/or legal obligations
- Requests from regulatory authorities

- Investigations by authorised bodies
- Coroners' investigations
- Fraud prevention
- When disclosure is necessary to protect someone from serious harm
- When disclosure is otherwise authorised by law

Changes introduced by the Data (Use and Access) Act 2025

The Data (Use and Access) Act 2025 (DUAA) amended UK data protection and privacy legislation. Whilst this new Act does not replace the Data Protection Act 2018 and UK GDPR, it has modified them. This organisation will maintain its policies and procedures in accordance with the legislation as amended by DUAA.

The DUAA gained Royal Assent on 19 June 2025 and started to be introduced from then. It is now fully in force.

Registering for NHS care

All patients who receive NHS care are registered on a national database (NHS Spine). The Spine is held and maintained by NHS England which has legal responsibilities to collect NHS data. Further information can be found in this YouTube clip from NHS England titled What is the NHS Spine?

How do we keep your information and how long do we keep it for?

Your personal information and health records are stored securely within the clinical and document management systems used by the practice.
We use **EMIS** as our clinical system to record and manage patient information, including clinical records, consultations, medications, test results and other information relevant to your care.
We also use **Docman** for the secure management, storage and processing of clinical documents and correspondence relating to your care.
These systems are provided by third-party organisations acting on behalf of the practice. Where we use third-party providers to store or process personal information, we ensure that appropriate contractual, technical and organisational measures are in place to protect your information and that the processing complies with UK data protection law.

Access to your information is restricted to authorised staff and other appropriate healthcare professionals who require it for legitimate purposes, such as providing your care, managing practice services or meeting our legal and regulatory obligations.
We retain your personal information in accordance with applicable NHS records management requirements and our legal and regulatory obligations.

This organisation will retain your medical records in accordance with NHS England's Records Management Code of Practice. Retention periods depend on the type of record and information will be disposed of by securely. We use Shred it to securely dispose of confidential waste.

Opting out of sharing your data

There are two types of opting out and below details both and the actions required should you wish to opt-out of sharing your data.

Type	Description	Actions
Type 1 Opt-out	This is to stop identifiable, or confidential information held in your GP record being disclosed outside the GP practice for purposes other than your individual care. NHS guidance titled Opt out of sharing your health records and also Summary Care Record	Contact the organisation and this will be locally coded into your clinical record.
National Data Opt-out **(NDO-O)**	This is to stop confidential patient information being used for certain research and planning purposes by NHS and other healthcare organisations. Refer to the following NHS guidance: • Make your choice about sharing data from your health records • National Data Opt-Out • Setting or changing a national data opt-out choice	Contact NHS England to opt-out. This action cannot be completed by the organisation

Sharing information for direct care – Type 1 Opt Out

Type 1 Opt-out applies at practice level and means that a patient's medical record is not extracted from the organisation for any purpose other than for direct patient care. Patients can opt-out at any time, and opting out will mean that no further extractions will be taken from the medical

record. It should be noted that sharing information between healthcare professionals is often necessary to provide safe and effective care and examples when sharing information is required include:

- Between the GP record and a hospital treating you
- Sharing relevant information with an out-of-hours service
- Providing medication information to another healthcare professional
- Sharing information with community nursing services
- Sharing relevant information with social care where necessary to coordinate care

Whilst it is the patient's decision as to whether this information is shared or not, there are benefits when another NHS organisation has limited healthcare information about a patient. Instances would include within an emergency setting or during an out of hours conversation about a patient's care. The limited information would be any current medication, allergies or reactions to medication and specific information to confirm the patient's details such as name, address, date of birth and NHS number. Having this information ensures that safer care is delivered.

When you object to sharing information for your individual care, this organisation will consider your objection, although there may be circumstances when information must nevertheless be shared, for example when there is an overriding public interest or when sharing is necessary to prevent serious harm.

Opting out of data sharing for research and planning – National Data Opt-Out

The other form of opting out is when a patient requests that confidential information is not shared when for research and planning purposes. This is called the National Data Opt-Out (NDO-O) and patients are able to opt-out at any time. Further information on medical research, audits and high-risk monitoring planning can be found below.

This opt-out cannot be completed by a GP practice as this has to be undertaken by the patient informing NHS England using any of the following methods:

Online	The NHS number and/or postcode is required. Further reading is at Make your choice about sharing data from your health records
Telephone	Call 0300 303 5678 between 0900 – 1700 Monday to Friday
NHS App	For use by patients aged 13 and over. The app can be downloaded from the App Store or Google Play
"**Print and post"**	To NHS England, PO Box 884, LEEDS, LS1 9TZ.

	Photocopies of proof of the applicant's name (e.g., passport, UK driving licence etc.) and address (e.g., utility bill, payslip etc.) will be needed and sent with the application. It should be noted that it can take up to 14 days to process the form. Patient information is available within the NHS guidance titled Manage your choice

Further information on NDO-O is available from the NHS England guidance:

- National Data Opt-Out
- Opt out of sharing your health records
- Make your choice about sharing data from your health records
- Sharing data from your health records – Information in different languages and formats

Safeguarding

- Sometimes we need to share information so that other people, including healthcare staff, children or others with safeguarding needs, are protected from risk of harm. These circumstances are rare, and we do not need your consent or agreement to do this.

Children and young people

When a young person is considered competent to make decisions about their healthcare, confidentiality will normally be respected. A parent or person with parental responsibility does not automatically have an unrestricted right to access a child's medical information.

Further reading can be found at:

- NHS England's guidance titled Children and young people
- Care Quality Commission's GP mythbuster 8: Gillick competency and Fraser guidelines
- The practices Privacy Notice – Easy read

People who lack capacity

When a person is considered to lack capacity to make a particular decision, information will be handled in accordance with the relevant legislation and guidance to ensure the best interests of the patient are always considered. Please note that a person acting under a Lasting Power of Attorney or other authority may not automatically have unrestricted access to all medical information and the scope of their authority will always be considered.

Artificial Intelligence (AI)

Prior to using AI, a full data protection impact assessment has been compiled by the organisation, and any AI use will comply with the strict data protection laws that also includes UK GDPR.

Clinicians are more frequently using AI software during consultations to support both the compiling and documenting of a patient's clinical record. There are two main types of personal data that will be processed during a consultation, including the patient's name, contact details, medical history, diagnosis, treatment information, and any other information shared during consultations. There may also be an audio recording of the clinician, although this is to detail their professional identifiers, such as name and title. Prior to any use of this technology within the consultation, patients are to be informed. This is for both transparency and also to allow the ability for any patient to object to having AI technology within their consultation.

For further information, a privacy notice that specifically supports AI use is available upon request and the CQC has issued guidance titled GP mythbuster 109: Use of artificial intelligence (AI) in GP services.

Data breaches

Loss of personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data, and this organisation will act upon a suspected data breach as soon as practicable following becoming aware of it. Data breaches will be reported to the Information Commissioner's Office (ICO) should it meet its threshold and in accordance with its guidance titled Personal data breaches: a guide. In addition to reporting to the ICO, should a data breach occur, then this is also reported to both the Department of Health and Social Care and NHS England.

Following any data breach there will be an investigation that supports lessons learned to prevent any reoccurrence.

Data complaints

Should you believe that there has been a breach of your data, then you can either complain to the organisation directly or to the Integrated Care Board. Should you be dissatisfied with the initial response, then you may then direct your complaint to the Information Commissioner's Office (ICO) by referring to How to deal with data protection complaints or, as for any other complaint, you may wish to escalate your complaint to the Parliamentary and Health Service Ombudsman.

Guidance on the complaints procedure can be found in the Practice Complaints Leaflet. Further reading to support the changes following the implementation of the Data (Use and Access) Act 2025 can be found in:

- NHS England document titled Personal data breaches and related incidents
- ICO guidance titled How to make a data protection complaint to an organisation

Review of this notice

As for all policies and procedures, this organisation will routinely review this privacy notice to ensure that the information is current. This is normally at least annually, or when there is a significant change in legislation, or guidance from the ICO, Government, or NHS England. Furthermore, this organisation will review this notice should there be a significant change in new systems or ways of working.

The organisation will maintain a version history.

Key information

This organisation is lawfully required to provide you with the following information about how we handle your information:

Data Controller	Elizabeth Heimes Practice Manager The Birches Medical Centre
Data Protection Officer	Shavarnah.purves@nhs.net
Purpose of the processing	To give direct health or social care to individual patients. An example is, when a patient agrees to a referral for direct care, such as to a hospital, relevant information about the patient will be shared with the other healthcare staff to enable them to give appropriate advice, investigations, treatments and/or care. To check and review the quality of care. This is called audit and clinical governance. Medical research and to check the quality of care which is given to patients. This is called national clinical audit.
Lawful basis for processing	These purposes are supported under the following sections of the GDPR: ***Article 6(1)(c)*** *'…necessary for compliance with a legal obligation to which the controller is subject'; and* ***Article 6(1)(e)*** *'…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'; and*

	Article 9(2)(h) *'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 or social care systems and services..."* The following sections of the GDPR mean that we can use medical records for research and to check the quality of care (national clinical audits): ***Article 6(1)(e)*** *– 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'.* For medical research: there are two possible Article 9 conditions. ***Article 9(2)(a)*** *– 'the data subject has given explicit consent…'* OR ***Article 9(2)(j)*** *– 'processing is necessary for… scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member States law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject'.*
Common law duty of confidence and the Caldicott Principles	Healthcare staff will also respect and comply with their obligations under the common law duty of confidence and in accordance with the eight Caldicott Principles: 1. Information is used only when necessary 2. Information is used only when necessary for a specified purpose 3. Information is used when necessary but only the minimum necessary is used 4. Access is limited to those who need it 5. Everyone with access understands their responsibilities 6. Compliance with the law is understood and complied with 7. The duty to share information for individual care is as important as the duty to protect confidentiality 8. Information is used in ways that people can understand and reasonable expectations are met The Caldicott Principles apply to confidential information used within health and social care and when information is shared between organisations. This organisation will also consider the Caldicott Principles when deciding whether information is shared between other healthcare organisations.

Recipient or categories of recipients of the processed data	The data will be shared with: • Healthcare professionals and staff in this surgery • Local hospitals including emergency departments and ambulance services • Out of hours services • Diagnostic and treatment centres • Other organisations involved in the provision of direct care to individual patients For medical research, the data will be shared if the patient has given consent. For national clinical audits that check the quality of care, the data will be shared with NHS England.
Rights to object and the national data opt-out	You have the right to object to information being shared between those who are providing you with direct care. This may affect the care you receive – please speak to the organisation. You are not able to object to your name, address and other demographic information being sent to NHS England. This is necessary if you wish to be registered to receive NHS care. You are not able to object when information is legitimately shared for safeguarding reasons. In appropriate circumstances, it is a legal and professional requirement to share information for safeguarding reasons. This is to protect people from harm. The information will be shared with the local safeguarding service. The national data opt-out model provides an easy way for you to opt-out of information that identifies you being used or shared for medical research purposes and quality checking or audit purposes. Please contact the organisation if you wish to opt-out. Guidance is available from NHS England's webpage titled National Data Opt-Out.
Right to access and correct	You have the right to access your medical record and have any errors or mistakes corrected. Please speak to a member of staff or look at our Access to Medical Records Policy. We are not aware of any circumstances in which you will have the right to delete correct information from your medical record although you are free to obtain your own legal advice if you believe there is no lawful purpose for which we hold the information and contact us if you hold a different view.

Retention period	Records will be kept in line with the law and national guidance. Information on how long records are kept for can be found in the NHS England guidance titled Records Management Code of Practice.
Right to complain	In the unlikely event that you are unhappy with any element of our data processing methods, do please contact the Practice Manager in the first instance. If you feel that we have not addressed your concern appropriately, you have the right to lodge a complaint with the Information Commissioner's Office (ICO) or, as for other types of level 2 complaints, alternatively you may wish to escalate your complaint to the Parliamentary and Health Service Ombudsman. For further details, visit the ICO webpage titled For the public and select "Make a complaint" or select the Live Chat option, or telephone: 0303 123 1113.
Data we get from other organisations	We receive information about your health from other organisations that are involved in providing you with health and social care. For example, if you go to hospital for treatment or an operation the hospital will send us a letter to let us know what has happened. This means your GP medical record is kept up to date when you receive care from other parts of the health service.

Annex C – Opt-out guidance for staff

This guidance is provided to all staff who may be required to respond to queries about the current data opt-outs available.

Who is NHS England?

NHS England is the national information and technology partner for the health and care system. It provides information and data to the health service so that it can plan effectively and monitor progress, create and maintain the technological infrastructure that keeps the health service running and links systems together to provide seamless care and develops information standards that improve the way different parts of the system communicate

NHS England is the national custodian for health and care data in England and has responsibility for standardising, collecting, analysing, publishing and sharing data and information from across the health and social care system, including general practice

What does it do with the data it collects?

Patient data collected from general practice is needed to support a wide variety of research and analysis to help to run and improve health and care services. While the data collected in other care settings such as hospitals is valuable in understanding and improving specific services, it is the patient data in general practice that helps NHS England to understand whether the health and care system as a whole is working for patients.

Furthermore, it may be used for research purposes or to analyse healthcare inequalities.

What type of data does NHS England extract from the organisation?

- Diagnoses and symptoms
- Observations
- Test results
- Medications
- Allergies and immunisations
- Referrals, recalls and appointments
- The patient's sex, ethnicity and sexual orientation
- Data about staff who have treated the patient

How does a patient opt-out?

Type	Description	Actions
Type 1 Opt-out	This is to stop identifiable or confidential information held in your GP record being disclosed outside the GP practice for clinical purposes. Further reading: • Opt out of sharing your health records • Summary Care Record	Contact the organisation and this will be locally coded into your clinical record.

National Data Opt-out **(NDO-O)**	This is to stop confidential patient information being used for certain research and planning purposes by NHS and other healthcare organisations. Further reading: • Make your choice about sharing data from your health records • National Data Opt-Out • Setting or changing a national data opt-out choice	Contact NHS England to opt-out. This action cannot be completed by the organisation.

Suggested response templates to a patient following a request to opt-out

The following suggested response templates can be used in support when requests for opting out are received from the following sources:

- **SMS (text) message content template**

You can opt-out of your health information being shared with NHS England for planning and research before the commencement date.

- **Patient information for website template**

The way in which patient data gathering is done by NHS England is changing. There is currently a lot of information online and in the news about your choices and opting out of these collections. You can opt-out of your GP record being shared with NHS England for planning and research and this should be done before the commencement date.

- **Email response template**

Thank you for your email regarding the sharing of patient data and being able to opt-out of these collections. The NHS England GP Data extraction is a legally required activity for this organisation. However, you do have a right to opt-out of the sharing of your data for research and planning purposes.

NHS England provides a detailed guide for patients on how the information it extracts is used and how you can opt-out. This can be found at General Practice Data for Planning and Research (GPDPR).

Please be aware that there are two types of opt-out:

Type 1 Opt-out – applies at organisational level and means that the patient's medical record is not extracted from the organisation for any purpose other than for direct patient care.

If you wish to opt-out, please let us know.

National Data Opt-out (NDO-O) – allows data to be extracted by NHS England for its lawful purposes but it cannot share this information with anyone else for research and planning purposes.

If you wish to apply for NDO-O, you must do this directly with NHS England. You can do this in any of the following ways:

- **Online service**

  Patients registering have to know their NHS number or postcode. Guidance can be sought from Make your choice about sharing data from your health records.

- **Telephone service**

  Contact 0300 303 5678 (Monday to Friday between 0900 and 1700).

- **NHS App**

  The app can only be used by patients aged 13 and over. It can be downloaded from either App Store or Google Play.

- "**Print and post"**

  Complete the following document in the Manage your choice link. Photocopies of proof of the applicant's name (e.g., passport, UK driving licence etc.) and address (e.g., utility bill, payslip etc.) need to be sent with the application to:

  NHS England
  PO Box 884
  LEEDS
  LS1 9TZ

  Note, it can take up to 14 days to process the form.

- **Telephone message template**

We have received numerous enquiries about patient data being extracted by NHS England to be used for research and planning. You, as a patient, have the right to opt-out of your information being used in this way.

Further reading about this process can be found by visiting https://www.thebirchesmedicalcentre.co.uk/ or, if you do not have internet access, please speak with a member of our reception team who will be very happy to explain this to you.

- **Information in regard to opting out in different languages**

For information in other languages, refer to the NHS guidance titled Sharing data from your health records – Information in different languages and formats.

- **Opting out whilst in a secure setting**

Healthcare professionals are required to assist patients in prison or other secure settings to register an opt-out choice.

For patients detained in such settings, information is available in the NHS England guidance titled Guidance for detained and secure estates.

Coding the patient record

The following SNOMED CT codes are to be used in relation to either opting out or opting back in:

Request	Descriptor	SNOMED CT Code
Opt-out	Dissent from secondary use of general practitioner patient identifiable data (finding).	827241000000103
Opt-in	Dissent withdrawn for secondary use of general practitioner patient identifiable data (finding)	827261000000102