Brackley Medical Centre (the Practice)

Data Protection Privacy Notice for Patients Version 2.0 – May 2025

Introduction

For the purpose of applicable data protection legislation including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, the GP practice responsible for your personal data is Brackley Medical Centre.

We, Brackley Medical Centre, will be known as the 'Controller' of the personal data you provide to us.

Your privacy is important to us, and we are committed to protecting and safeguarding your data privacy rights.

This Privacy Notice applies to personal information processed by or on behalf of the Practice. It applies to the personal data of our patients and to the data you have given us about your carers/family members. It covers the following topics:

- Why do we need your data?
- What data do we collect about you?
- What is the legal basis for using your data?
- How do we store your data?
- How do we maintain the confidentiality of your data?
- How long do we keep your data?
- What are your data protection rights?
- Who do we share your data with?
- Are there other projects where your data may be shared?
- When is your consent not required?
- How can you access or change your data?
- What should you do if your personal information changes?
- Changes to our privacy policy
- Our Data Protection Officer
- How to contact the appropriate authorities

Why do we need your data?

As your General Practice, we need to know your personal, sensitive and confidential data in order to provide you with appropriate healthcare services. Your records are used to facilitate the care you receive, and to ensure you receive the best possible healthcare.

Information may be used within the GP practice for clinical audit, to monitor the quality of the service provided.

What data do we collect about you?

Personal data: We collect basic personal data about you which does not include any special types of information or location-based information. This includes your name, postal address and contact details such as email address and telephone number.

By providing the Practice with your contact details, you are agreeing to the Practice using those channels to communicate with you about your healthcare, i.e. by letter (postal address), by voice-mail or voice-message (telephone or mobile number), by text message (mobile number) or by email (email address). If you are unhappy or have a concern about our using any of the above channels, please let us know.

Special Category personal data: We also collect confidential data linked to your healthcare which is known as "special category personal data", in the form of health information, religious belief (if required in a healthcare context) ethnicity and gender. This is obtained during the services we provide to you and through other health providers or third parties who have provided you with treatment or care, e.g. NHS Trusts, other GP surgeries, Walk-in clinics etc.

Records which the Practice holds about you may include the following information:

- Details about you, such as your address, carer, legal representative, emergency contact details
- Any contact the Practice has had with you, such as appointments, clinic visits, emergency appointments etc.
- Notes and reports about your health
- Details about your treatment and care
- Results of investigations such as laboratory tests, x-rays etc
- Relevant information from other health professionals, relatives or those who care for you

NHS records may be electronic, on paper, or a mixture of both.

Use of CCTV: Closed circuit television is utilised to protect the safety of our patients, staff and members of the public. To maintain privacy and dignity, CCTV is not in place where examinations or procedures are being undertaken. The Practice remains the data controller of this data and any disclosures or requests should be made to the Practice Manager.

Special Provisions for Children's Data

We have specific processes for handling children's personal data, recognising that additional care is required for this sensitive information.

Parental Access and Control

- Parents/guardians can generally access their child's records if the child is under 13 years old
- For children aged 13-15, we assess capacity on a case-by-case basis to determine whether the child can provide consent or if parental involvement is needed

- From age 16, young people are presumed to have capacity to consent to their own healthcare and data processing, unless proven otherwise

Safeguards for Children's Data

- We apply enhanced security measures to all children's records
- Access to children's records is restricted to staff with specific roles in paediatric care
- We are particularly vigilant in protecting children's data in safeguarding situations
- We provide age-appropriate information about data processing when communicating directly with children

Legal Basis for Processing Children's Data

We process children's data under the same legal basis as adult data, with additional considerations for their specific needs and vulnerabilities:

- Article 6(1)(e) of the UK GDPR - public task/official authority
- Article 9(2)(h) of the UK GDPR - provision of health or social care
- Consideration of the "best interests of the child" is paramount in all processing activities

What is the legal basis for using your data?

We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- Data Protection Act 2018
- The UK General Data Protection Regulations 2018
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Health and Social Care Act 2012
- NHS Codes of Confidentiality, Information Security and Records Management

Under the UK General Data Protection Regulation we will lawfully be using your information in accordance with:

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"

Article 9(2)(h) - "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"

For the processing of special categories data, the basis is:

Article 9(2)(b) – "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law"

These articles apply to the processing of information and the sharing of it with others for specific purposes.

How do we store your data?

We have a Data Protection regime in place to oversee the effective and secure processing of your personal and special category (sensitive, confidential) data. No third parties have access to your personal data unless the law allows them to do so and appropriate safeguards have been put in place.

Technical and Organisational Security Measures

We implement a variety of security measures to maintain the safety of your personal information, including:

- Encryption of electronic medical records
- Secure networks with firewalls and intrusion detection systems
- Regular security testing and assessments
- Physical security measures for our premises
- Regular data protection audits
- Business continuity and disaster recovery plans
- Secure disposal of confidential waste

TPP SystmOne

The Practice uses TPP SystmOne as our clinical system to manage your medical records. SystmOne is a highly secure electronic patient record system that helps us deliver efficient and effective healthcare. Key features include:

- Strict role-based access controls to ensure only authorised staff can access specific information
- Full audit trails that record every access to patient information
- Secure sharing capabilities with other healthcare providers when required for your care
- Advanced encryption to protect your data both when stored and when transmitted
- Regular security updates and patches to address emerging threats
- Integration with NHS systems like the NHS Spine and Electronic Prescription Service

TPP, the provider of SystmOne, acts as a data processor on behalf of the Practice and has rigorous security measures in place to protect patient information in accordance with UK data protection laws.

In certain circumstances you may have the right to withdraw your consent to the processing of data. These circumstances will be explained in subsequent sections of this document.

In some circumstances we may need to store your data after your consent has been withdrawn, in order to comply with a legislative requirement.

Remote Consultations and Telehealth

Brackley Medical Centre offers remote consultation options including telephone and video consultations. These services allow you to receive care without needing to visit the practice in person.

How We Process Data During Remote Consultations

When you participate in a remote consultation:

- We use secure, NHS-approved platforms for video consultations
- Consultations are not routinely recorded unless specifically required for your care, and only with your explicit consent
- The same standards of confidentiality and data protection apply as for in-person consultations
- Notes and records from remote consultations are stored in your medical record just like in-person appointments
- We may process information about your device and internet connection (such as IP address) for technical purposes only
-

Third Parties Involved in Remote Consultations

Our remote consultation services may be supported by third-party providers who act as data processors. These providers:

- Have formal data processing agreements in place
- Process data only according to our instructions
- Implement appropriate technical and organisational measures to protect your data
- Do not use your data for their own purposes
- Comply with UK GDPR and NHS Digital requirements

Legal Basis for Remote Consultations

We process your data for remote consultations under the same legal basis as in-person care:

- Article 6(1)(e) of the UK GDPR - processing is necessary for the performance of a task carried out in the public interest
- Article 9(2)(h) of the UK GDPR - processing is necessary for medical diagnosis and the provision of healthcare

How do we maintain the confidentiality of your data?

Our Practice policy is to respect the privacy of our patients, their families and our staff and to maintain compliance with the UK General Data Protection Regulations (UK GDPR) and all UK specific Data Protection requirements. Our policy is to ensure all personal data related to our patients will be protected.

We use a combination of working practices and technology to ensure that your information is kept confidential and secure.

Every member of staff who works for an NHS organisation has a legal obligation to keep information about you confidential.

Staff Training

All staff at Brackley Medical Centre receive regular training on data protection and information governance. This training covers:

- UK GDPR and Data Protection Act 2018 requirements
- Safe handling of personal and special category data
- Recognising and reporting data breaches
- Patient rights regarding their data
- Secure use of practice systems and technology
- Confidentiality obligations

Our staff are required to complete mandatory data protection training annually, and additional training when new systems or requirements are introduced.

All employees and sub-contractors engaged by our Practice are asked to sign a confidentiality agreement. The Practice will, if required, sign a separate confidentiality agreement if the client deems it necessary. If a sub-contractor acts as a data processor for Brackley Medical Centre an appropriate contract will be established for the processing of your information.

Some of this information will be held centrally and used for statistical purposes. Where this happens, we take strict measures to ensure that individual patients cannot be identified.

Sometimes your information may be requested to be used for research purposes. The Practice will always gain your consent before releasing the information for this purpose in an identifiable format. In some circumstances you can Opt-out of the Practice sharing any of your information for research purposes.

Use of AI Technologies

Brackley Medical Centre uses various AI (Artificial Intelligence) technologies to support healthcare delivery and administrative functions.

Heidi Health Scribe

Heidi Health Scribe is an advanced, secure digital assistant designed to support clinicians during consultations. It uses artificial intelligence to document medical notes, ensuring your clinician can focus on actively listening to your concerns and delivering personalised care, rather than spending time manually recording the notes. Clinicians review and approve the notes that have been captured prior to adding to the patient record. No decisions are made by Heidi, it simply helps to document your visits more effectively.

Claude AI

Brackley Medical Centre also uses Claude AI, an advanced artificial intelligence assistant developed by Anthropic, to support certain administrative and clinical documentation tasks. Claude AI is designed to assist our staff in processing information, drafting content, and enhancing our service delivery.

How Claude AI Works in Our Practice

Claude AI processes and generates text based on specific information it is given by our authorised staff. At our practice, Claude AI may be used for:

- Drafting standard letters and communications that are then reviewed by healthcare staff
- Creating first drafts of patient educational materials
- Summarising complex medical information into patient-friendly explanations
- Assisting with analysing anonymised healthcare data for service improvement
- Supporting staff with administrative documentation

Data Processing with Claude AI

When we use Claude AI:

- The system only processes the specific information that our staff input
- No direct patient identifiable information is retained by the AI system
- All outputs are always reviewed by qualified healthcare professionals before being finalised or shared
- The practice maintains full control over all data processed
- Use of Claude AI complies with NHS data protection and security standards

How Our AI Systems Work

Our AI systems like Heidi Health Scribe and Claude AI use speech recognition, natural language processing, and other AI technologies to support healthcare delivery. These systems help create clinical notes during consultations, draft communications, and analyse anonymised data to improve practice operations.

Data Processing with AI Systems

When we use AI systems:

- The AI may process audio recordings of your consultation, but these recordings are typically not stored long-term and are deleted once processing is complete
- Draft notes and content created by AI are always reviewed by our healthcare professionals before being finalised
- The data is processed securely in accordance with UK data protection laws and NHS security standards
- Your information is only used for the purpose of creating accurate medical records and improving our services
- All AI service providers are bound by strict data processing agreements and confidentiality requirements

Data Security for AI Systems

- Data Security: Our AI systems comply with UK data protection laws, including UK GDPR, ensuring that your information is handled securely and confidentially. All information is processed securely within our practice, and our AI providers do not store any patient information beyond what is necessary for processing.
- Data Protection Impact Assessments: Before implementing any AI system, we conduct thorough Data Protection Impact Assessments (DPIAs) to ensure all risks are identified and mitigated.
- Data Protection Officer Review: The AI systems we use have been reviewed and approved by the Data Protection Officer for Northamptonshire NHS Integrated Care Board.

Your Rights Regarding AI Processing

- You have the right to:
- Be informed that AI technology is being used in your consultation or for administrative purposes
- Request that AI systems not be used in your consultation or for processing your information
- Access the information that has been recorded about you
- Request correction of any inaccuracies in the information recorded
- Object to the use of AI in your care

If you prefer not to have AI systems involved in your care, please let your clinician know. This will not affect the quality of care you receive.

How long do we keep your data?

We are required under UK law to keep your information and data for the full retention periods as specified by the NHS Records Management Code of Practice for Health and Social Care and in accordance with National Archives requirements.

More information on records retention can be found online at: https://transform.england.nhs.uk/media/documents/NHSX_Records_Management_CoP_V7.pdfh

What are your data protection rights?

If we already hold your personal data, you have certain rights in relation to it.

Right to be informed: You have the right to be informed on how we handle, process, and share your personal information.

Right to access your personal information: You can request access to and/or copies of the personal data we hold about you, free of charge (subject to exemptions) within one calendar month.

Right to object: If we are using your data because we deem it necessary for our legitimate interests to do so, and you do not agree, you have the right to object. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases). Generally, we will only disagree with you if certain limited conditions apply.

Right to withdraw consent: Where we have obtained your consent to process your personal data for certain activities (for example a research project), or consent to market to you, you may withdraw your consent at any time.

Right to erasure: In certain situations (for example, where we have processed your data unlawfully), you have the right to request us to erase your personal data. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply.

Right of data portability: If you wish, you have the right to transfer your data from us to another data controller. We will help with this with a GP-to-GP data transfer and transfer of your hard copy notes.

To exercise any of these rights, please contact our Data Protection Officer or Practice Manager.

Data Provision Notice sharing information with NHS Digital

The Practice is required to comply with the Health and Social Care Act 2012. NHS Digital have the power under the Health and Social Care Act 2012 Section 259 (1) to issue a Data Provision Notice. This mandates us to share information about you unless you tell us not to.

You can see a list of the Data Provision Notices here: https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/data-provision-notices-dpns

National Data Opt-Out: The National Data Opt-Out is a service that allows people to opt out of their confidential patient information being used for research and planning purposes. The National Data Opt-Out replaces the previous Type 2 Opt-Out, which required NHS Digital not to share a patient's confidential patient information for purposes beyond their individual care.

If a patient wants to change their choice, they can use the service to do this. You can find out more from the Practice or by visiting: https://www.nhs.uk/your-nhs-data-matters/

If you wish to raise a query or request relating to any of the above, please contact us. We will seek to deal with it without undue delay, and in any event in accordance with the requirements of any applicable laws. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

Who do we share your data with?

We consider patient consent as being the key factor in dealing with your health information.

To provide around-the-clock safe care, we will make information available to trusted organisations for specific purposes unless you have asked us not to.

To support your care and improve the sharing of relevant information to our partner organisations when they are involved in looking after you, we will share information to other systems. The general principle is that information is passed to these systems unless you request that this does not happen, but that system users should ask for your consent before viewing your record.

Our partner organisations are:

- NHS Trusts / Foundation Trusts
- GPs
- NHS Commissioning Support Units
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers
- Ambulance Trusts
- Clinical Commissioning Groups
- Social Care Services
- NHS England (NHSE) and NHS Digital (NHSD)
- Multi Agency Safeguarding Hub (MASH)
- Local Authorities
- Education Services
- Fire and Rescue Services
- Police and Judicial Services

- Voluntary Sector Providers
- Private Sector Providers
- Other 'data processors' which you will be informed of

You will be informed who your data will be shared with, and in cases where your consent is required you will be asked for it.

Below are some examples of when we would wish to share your information with trusted partners.

Primary Care Networks: We are a member of Brackley & Towcester Primary Care Network. This means we work closely with a number of local practices and care organisations for the purpose of direct patient care. They will only be allowed to access your information if it is to support your healthcare needs. If you have any concerns about how your information may be accessed within our primary care network, we would encourage you to speak or write to us.

Extended Access: We provide extended access services to our patients which means you can access medical services outside of our normal working hours. In order to provide you with this service, we have formal arrangements in place with the Clinical Commissioning Group and with other practices whereby certain key "hub" practices offer this service on our behalf for you as a patient to access outside our opening hours. Those key "hub" practices will need to have access to your medical record to be able to offer you the service. We have robust data sharing agreements and other clear arrangements in place to ensure your data is always protected and used for those purposes only.

Medicines Management: The Practice may conduct Medicines Management Reviews of medications prescribed to its patients. This service performs a review of prescribed medications to ensure patients receive the most appropriate, up-to-date and cost-effective treatments. Our local NHS Clinical Commissioning Group employs specialist pharmacists and they may at times need to access your records to support and assist us with prescribing. This reason for this is to help us manage your care and treatment.

Individual Funding Requests: An Individual Funding Request is a request made on your behalf, with your consent, by a clinician, for the funding of specialised healthcare which falls outside the range of services and treatments that CCG has agreed to commission for the local population. An Individual Funding Request is considered when a case can be set out by a patient's clinician that there are exceptional clinical circumstances which make the patient's case different from other patients with the same condition who are at the same stage of their disease, or when the request is for a treatment that is regarded as new or experimental and where there are no other similar patients who would benefit from this treatment. A detailed response, including the criteria considered in arriving at the decision, will be provided to the patient's clinician.

Are there other projects where your data may be shared?

GP Data Sharing Project with NHS East Midlands Ambulance Service: The Practice is working with the local ambulance service trust, NHS East Midlands Ambulance Service, to share your healthcare information for the purposes of your care and treatment. They can only access your information if it is for care purposes. If you have any concerns, please speak to the Practice.

GENVASC: NHS Arden and Greater East Midlands CSU (AGEM CSU) support the Practice in providing information to the GENVASC Research Study. AGEM CSU will securely extract data from the Practice system. They will then provide the GENVASC Study with the agreed information relating to patients who have signed a GENVASC Research Study consent form. Please note that AGEM CSU operate under the instructions of the Practice at all time and have processes and safeguards in place to ensure the confidentiality and security of all information at all times. If further information is required please contact the GENVASC study team at NIHR Leicester Biomedical Research Centre Cardiovascular theme on 0116 2583385 or visit www.genvasc.uk

Local Research: We regularly work with local health and academic organisations to conduct research studies with the aim of improving care for the general population. We will always ask for your permission to take part, except in situations where we can demonstrate that your information has been anonymised (where you cannot be identified) and your privacy is protected. In these situations we are not required to seek consent from individuals.

Call Recording: The Practice records all telephone calls. This is done so that we have a record of conversations we have with you, staff and healthcare workers are protected from potential abuse. If you would like a copy of call recording which are you are the data subject for you are entitled to ask for a copy of this.

COVID-19 Data Processing

During the COVID-19 pandemic, it has been necessary to share confidential patient information to respond to the outbreak effectively. The Secretary of State for Health and Social Care used powers under the Health Service (Control of Patient Information) Regulations 2002 to require organisations to process confidential patient information for COVID-19 purposes.

This processing includes:

- Understanding COVID-19 risks and controlling them
- Identifying and protecting those who may be vulnerable to COVID-19
- Delivering services to patients, clinicians, and the public
- Supporting research into COVID-19 and planning during the pandemic

The legal notices requiring this processing were initially to expire on 30th September 2020 but were extended to ensure ongoing protection during the pandemic. This privacy notice

will be updated as the situation evolves.During this period of emergency, opt-outs have not generally applied to the data used to support the COVID-19 outbreak, due to the public interest in sharing information. However, we have continued to process normal opt-out requests for all other purposes of data sharing.

Risk Stratification

Risk stratification data tools are increasingly being used in the NHS to help determine a person's risk of suffering a condition, preventing an unplanned admission or re-admission and identifying a need for preventive intervention. Information about you is collected from a number of sources including NHS Trusts and from this GP practice. A risk score arrived at through an analysis of your de-identified information is provided back to your GP practice as data controller in an identifiable form. Risk stratification enables your GP to focus on preventing ill health and not just the treatment of sickness. If necessary, your GP may be able to offer you additional services. Please note that you have the right to opt out of your data being used in this way.

Other research projects

With your consent we would also like to use your name, contact details and email address to inform you of services that may benefit you. There may be occasions when authorised research facilities would like to invite you to participate in research, innovations, identifying trends or improving services. At any stage where we would like to use your data for anything other than the specified purposes and where there is no lawful requirement for us to share or process your data, we will ensure that you have the ability to consent or to opt out prior to any data processing taking place. This information is not shared with third parties or used for any marketing and you can unsubscribe at any time via phone, email or by informing the Practice.

When is your consent not required?

We will only ever use or pass on information about you to others involved in your care if they have a genuine need for it. We will not disclose your information to any third party without your permission unless there are exceptional circumstances.

There are certain circumstances where we are required by law to disclose information, for example:

- where there is a serious risk of harm or abuse to you or other people
- where a serious crime, such as assault, is being investigated or where it could be prevented
- notification of new births
- where we encounter infectious diseases that may endanger the safety of others, such as meningitis or measles (but not HIV/AIDS)
- where a formal court order has been issued
- where there is a legal requirement, for example if you had committed a Road Traffic Offence

We are also required to act in accordance with Principle 7 of the Caldicott Review (Revised version 2013) which states: "The duty to share information can be as important as the duty to protect patient confidentiality." This means that health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott Principles.

Accessibility

We are committed to ensuring this Privacy Notice is accessible to everyone. If you would like this Notice in another format (for example: audio, large print, braille) please contact us.

How can you access or change your data?

You have a right under the Data Protection legislation to request access to view or to obtain copies of the information the Practice holds about you and to have it amended should it be inaccurate.

Your request should be made to the Practice and we have a form (SAR - Subject Access Request) which you will need to complete. We are required to respond to you within one calendar month.

For information from the hospital you should write direct to them. You will need to give adequate information (full name, address, date of birth, NHS number and details of your request) so that your identity can be verified and your records located.

There is no charge to receive a copy of the information held about you.

What should you do if your personal information changes?

Please contact the Practice Manager as soon as any of your details change. This is especially important for changes of address or contact details (such as your mobile phone number). The Practice will from time to time ask you to confirm that the information we currently hold is accurate and up-to-date.

Changes to our privacy policy

It is important to point out that we may amend this Privacy Notice from time to time.

Our Data Protection Officer

The Practice has appointed: Midlands and Lancashire Commissioning Support Unit

They can be contacted on the following e-mail address: mlcsu.dpo@nhs.net or general IG and Primary Point access queries: mlcsu.ig@nhs.net

Midlands and Lancashire Commissioning Support Unit
Heron House, 120 Grove Road
Fenton
Stoke-on-Trent
ST4 4LX

If you have any concerns about how your data is shared, or if you would like to know more about your rights in respect of the personal data we hold about you, then please contact the Practice Manager.

How to contact the appropriate authorities

If you have any concerns about how your information is managed at your GP Practice, please contact the GP Practice Manager or the Data Protection Officer in the first instance.

If you are still unhappy following a review by the GP Practice, you have a right to lodge a complaint with the UK supervisory authority, the Information Commissioner's Office (ICO), at the following address:

Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 01625 545745
Email: https://ico.org.uk/