Privacy Statement

Brunton Park Health Centre
Princes Road
Gosforth
Newcastle upon Tyne
NE3 5NF

Practice Manager: Kay Wannop

Telephone: 0191 2363338

ICO Registration No:Z6615851

Data Protection Officer: Liane Cotterill

Email: NECSU.IG@nhs.net

Introduction

This document has been created to explain to you the types of personal data Brunton Park Health Centre holds about you and how we may use this information for the benefit of your health and wellbeing. The document advises you on how we allow your health record to be made available to other organisations, across a variety of healthcare and other settings.

How we use your information

Brunton Park Health Centre aims to ensure the highest standard of medical care for our patients. To do this we keep records about you, your health and the care we have provided or plan to provide to you. This document outlines how that information is used, with whom we may share that information, how we keep it secure (confidential) and what your rights are in relation to this.

The Health Care Professionals (HCP) who provide you with care, maintain records about your health and any treatment or care you have received previously (e.g. NHS Trust, GP surgery, Community clinics or staff etc.). These records help to provide you with the best possible healthcare, and:

- Provide a basis for all health decisions made by HCPs with and for you;
- Make sure your care is safe and effective;
- Work effectively with others providing you with care.
- Send you text notifications to you about appointment reminders or cancellation of clinics. You can opt out of the text notification service at any time by phoning the practice on 01912363338.

NHS health records may be electronic, on paper or a mixture of both and we use a combination of working practices and technology to ensure that your information is kept confidential and secure.

What kind of information do we use?

As your registered GP practice, we hold your electronic health record. This contains sensitive information about you, your health and your wellbeing. The following list provides an example of the type of information (both past and present) that can be held within your record:

- Demographic details about you and contact details (name, date of birth, address, telephone number, email address, gender, sex, religion, marital status etc.)

- Any contact the surgery has had with you such as appointments, clinic visits, emergency appointments, consultations and so on
- Notes and reports about your health
- Details about your treatment and care including diagnoses (this can include physical disabilities and mental health conditions)
- Medication, vaccinations, pathology results (e.g. blood tests) and allergies
- Social care involvement
- Results and investigations
- Hospital correspondence and correspondence from other health and social care settings (including x-rays, discharge letters and referrals)
- Relevant information from other HCPs, relatives or those who care for you
- Relationships/next of kin/carer information etc.

To ensure you receive the best possible direct care, your records are used to facilitate the care you receive. Information held about you may be used to help protect the health of the public and to help us manage the NHS. Information may be used for clinical audit to monitor the quality of the service provided and to plan NHS services.

Some of this information will be held centrally and used for statistical purposes, such as NHS performance and activity. Where we do this, 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 organisation will always endeavor to gain your consent before releasing the information.

Information may be requested for financial validation and Care Quality Commission purposes. Where we do this, we take strict measures to ensure that individual patients cannot be identified. During Care Quality Commission inspections, the inspectors are required to review random patient records.

We may also process your information when investigating concerns, complaints or legal claims. It could also be used to help staff to review the care they provide to make sure it is of the highest standards, training and educating staff.

The NHS Care Record Guarantee for England sets out the rules that govern how patient information is used in the NHS and what control patients can have over this.

The NHS Constitution https://www.gov.uk/government/publications/the-nhs-constitution-for-england establishes the principles and values of the NHS in England. It sets out rights to which patients, public and staff are entitled, and pledges which the NHS is committed to achieve, together with responsibilities, which the public, patients and staff owe to one another to ensure that the NHS operates fairly and effectively.

What do we mean by direct care?

The term 'direct care' means a clinical health activity concerned with the prevention and investigation and treatment of illness. It includes supporting your ability to function and improve your participation in life and society. It also includes the assurance of safe and high quality care and treatment undertaken by one or more registered and regulated health or social professionals and their team with whom you have a legitimate relationship for your care purposes.

What do we use your personal and confidential/sensitive information for?

We are committed to protecting your privacy and will only use information that may identify you (known as personal information) in accordance with the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), the Data Protection Act 2018, other laws such as the Health and Social Care Act 2012. http://www.legislation.gov.uk/ukpga/1998/29/contents and http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted, and Article 8 of the Human Rights Act, however only the minimum necessary identifiers are used in processing personal information for the purpose. We also have a Common Law Duty of Confidentiality to protect your information. This means that where a legal basis for using your personal or confidential information does not exist, we will not do so.

Apart from direct health care sensitive personal information (including special categories of data) may also be used in the following cases:

- To respond to patients, carers or Member of Parliament communication.
- We have received consent from individuals to be able to use their information for a specific purpose.
- There is an over-riding public interest in using the information e.g. in order to safeguard an individual, or to prevent a serious crime.
- There is a legal requirement that will allow us to use or provide information (e.g. a formal court order, notification of infectious disease).
- For the health and safety of others, for example to report an infectious disease such as meningitis or measles.
- We have special permission for health and research purposes (granted by the Health Research Authority).
- We have special permission called a 'section 251 agreement' (Section 60 of the Health and Social Care Act 2001 as re-enacted by Section 251 of the NHS Act 2006) which allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes. An example of where this is used is in risk stratification. Further information can be found on the Health Research Authority's web site here http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/what-is-section-251/

Legal basis

The Legal basis for the processing health data is covered under Article 6 (1)(e) of the General Data Protection Regulation where "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" and Article 9 (2)(h) where "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 or social care systems and services on the basis of Union Or Member State law or pursuant to contract with a health professional…".

Where there is a need for information to be processed in the interests of the health and safety of others, for example to report an infectious disease such as meningitis or measles, the legal basis under GDPR is Article 6 (1)(c) '….for compliance with a legal obligation….', and Article 9 (2) (h) as above.

Where consent from individuals is required the legal basis is Article 6 (1) (a), 'the data subject has given consent to the processing of his or her personal data for one or more specific purposes' and

Article 9 (2) (a) ' the data subject has given explicit consent to the processing of those personal data for one or more specified purposes…'.

We have special permission to processing information for health and research purposes the legal basis is Article 6 (1) (e) as above, and Article 9 (2) (j) '….research purposes…'.

How do we maintain confidentiality of your records?

We are committed to protecting your privacy and will only use information collected lawfully in accordance with the General Data Protection Regulation (Regulation (EU) 2016/679), Data Protection Act 2018 (which is overseen by the Information Commissioner's Office), Human Rights Act, the Common Law Duty of Confidentiality and the NHS Codes of Confidentiality and Security.

Every member of staff who works for an NHS organisation has a legal obligation to keep information about you confidential. Anyone who received information from an NHS organisation has a legal duty to keep it confidential. All persons in the practice sign a confidentiality agreement that explicitly makes clear their duties in relation to personal information and data concerning health, and the consequences of breaching that duty.

Please be aware that your information will be accessed by non-clinical practice staff in order to perform tasks enabling the functioning of the practice. These are, but not limited to:

- Typing referral letters to hospital consultants or other HCPs.
- Opening letters from hospitals and consultants.
- Scanning clinical letters, radiology reports and any other documents not available in electronic format.
- Photocopying or printing documents for referral to consultants.
- Handling, printing, photocopying and postage of medico legal and life assurance reports and of associated documents.

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

The NHS Digital Code of Practice on Confidential Information applies to all of our staff, and they are required to protect your information, inform you of how your information will be used, and allow you to decide if and how your information can be shared. All practice staff are expected to make sure information is kept confidential and receive annual training on how to do this. This is monitored by the practice and can be enforced through disciplinary procedures.

We also ensure the information we hold is kept in secure locations, restrict access to information to authorised personnel only and protect personal and confidential information held on equipment such as laptops with encryption (which masks data so that unauthorised users cannot see or make sense of it).

To protect your confidentiality, we will not normally disclose any medical information about you over the telephone, or by fax, unless we are sure that we are talking to you. This means that we will not disclose information to your family, friends and colleagues about any medical matters at all, unless we know that we have your consent to do so.

We ensure external data processors that support us are legally and contractually bound to operate and prove security arrangements are in place where information that could or does identify a person is processed.

We have a senior person responsible for protecting the confidentiality of patient information and enabling appropriate information sharing. This person is called the Caldicott Guardian. The Caldicott Guardian for the practice is Dr Glynn Malone. We also have a Senior Information Risk Owner (SIRO) who is responsible for owning the practice's information risk. The SIRO Dr G Malone. The Data Protection Officer for the practice is named at the top of this notice.

We are registered with the Information Commissioner's Office (ICO) as a data controller which describes the purposes for which we process personal data. A copy of the registration is available from the ICO's web site by searching on our practice name.

Sharing Information with Other Organisations

For Direct Care Purposes

Who are our Partner Organisations?

If you are referred to or attend another health or care organisation, we will share information with them in order that you receive the best and safest possible care. Examples of these organisations include:

- NHS Trusts
- NHS111
- Hospital Laboratories (when we send samples to the hospital lab, the results also become part of the hospital record and will be viewable by hospital staff if they are involved in your care now or in the future)
- Specialist Trusts
- Relevant GP Practices
- Urgent and Unscheduled Care (e.g. A&E Minor Injury Units (MIU))
- Community services (e.g. physiotherapy, diabetic clinics, district nursing, rehabilitation centres)
- Community pharmacy
- Child health
- Palliative care
- NHS mental health services
- Independent contractors such as dentists, opticians, pharmacists
- Private sector providers such as hospitals, care homes, hospices, contractors providing services to the NHS.
- Voluntary sector providers who are directly involved in your care
- Ambulance Trusts
- Local authority care services

EMIS Shared Record

This practice operates a clinical computer system, EMIS Web, on which NHS staff record information securely. EMIS is a UK based company and all our information is stored in data centres in the UK that meet or exceed Government security requirements. Only persons on the secure, dedicated NHS network can access EMIS.

To provide around the clock safe care, unless you have asked us not to, we will make information available to trusted organisations who also use EMIS Web locally. Wherever possible, staff will ask your consent before information is viewed.

The practice can also access the EMIS Shared Record to view other organisations' details. Wherever possible we will ask for your consent before viewing the shared record, but as your GP and therefore care co-ordinator, when you joined the practice there is implied consent for us to view information relevant to provide you with direct care.

You can opt out of the EMIS record sharing by informing the practice in writing, though this may affect the quality of care you receive if we cannot communicate effectively.

Summary Care Record (SCR)

The Summary Care Record is a national scheme linked to the spine to share information about the medicines you are prescribed and any allergies or other adverse reactions you have experienced. This information is uploaded to a central NHS database automatically from the GP clinical record.

The spine is also used in practice for electronic transportation of referral letters to the hospital and medication requests to your nominated pharmacy.

Health Professionals at other organisations will only be able to access this information with your permission. This might be important if you need urgent medical care when the GP practice is closed. When attending secondary care, GP OOH etc., your medical records will be accessed via the partner's own systems, which interface with the main NHS Spine and your own record which is held by the practice. NHS services can look at your SCR if they need to treat you when the practice is closed. They will ask for consent before they look at your records. In an emergency and if you are unconscious, staff may look at your SCR without your agreement to let them give you the best possible care. Whenever NHS staff look at your SCR, a record will be kept so we can always check who has looked at your information. The general principle is that information is passed to these systems unless you request this does not happen, but that system users should ask for your consent before viewing your records.

You have the right to opt-out of having a summary care record by informing the practice in writing, though this can place your health at risk if that information is not available in an emergency.

Great North Care record (GNCR)

A local initiative to share health and care information in the North East. The information shared is similar to that in the Summary Care Record with Additional Information. Unlike the Summary Care Record, no information is transferred out of the GP clinical system or stored elsewhere. In the future, the practice will also be able to view information in other health and care organisations' systems with your permission.

Health and Care Professionals at other organisations will only be able to access this information with your permission. More information about the GNCR and which organisations are involved can be found at: https://www.greatnorthcarerecord.org.uk/

Depending on their role, Health and Care Professionals can currently view:

- Demographic information
- Diagnoses and any other coded information
- Investigation Results
- Medication and allergies

They are unable to read consultation notes or any information that we have 'locked'. You can ask for any information you consider to be sensitive to be locked.

You have the right to opt-out of allowing the GNCR to view your record summary by informing the practice in writing, though this can place your health at risk if that information is not available in an emergency. Note also that opting-out of the GNCR will also result in opting out of the EMIS Shared Record – the two systems share the same opt out code.

Mail to Patients

We use a printing company called DocMail to send letters to our patients. Data is sent encrypted and the company puts it in a format to print the letter, dispatch via Royal Mail and then delete the information we send.

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. This service is provided by CBC Health Ltd, our parent organisation.

Telephone Call Recording

Brunton Park Heath Centre records incoming and outgoing telephone calls for training and monitoring purposes. These electronic sound files form part of your record and can provide useful information in the event of a complaint. Such recordings must be made, stored and disclosed under the provisions of the relevant legislation.
Under the provisions of the GDPR, you have a right to be provided with copies of information that is held about you and this includes recordings of telephone consultations. If you wish for telephone call not to be recorded we can remove your call but you must inform the Receptionist.

Sharing for Purposes Other than Direct Care

We may also have to share your information, subject to strict agreements on how it will be used, with the following organisations. This will be anonymised where possible:

- Offender health (care providers within organisations such as Prisons and Custody Suites)
- Clinical Commissioning Groups
- Social Care and Health
- Local Authorities
- Education Services
- Fire & Rescue Services
- General Medical Council
- Medical Indemnity Companies
- Police

- Other data processors

Who else may ask to access your information

The **court** can insist that we disclose medical records to them.

Solicitors also often ask for medical reports. These will always be accompanied by your signed consent for us to disclose information. We will not normally release details about other people that are contained in your records e.g. spouse, children, parent etc., unless we also have their consent.

Social Services may require medical reports on you from time to time. These will often be accompanied by your signed consent to disclose information. Failure to co-operate with these agencies can lead to loss of benefit or other support. However, if we have not received your signed consent we will not normally disclose information about you.

Other Government Departments such as the Department of Work and Pensions, or the DLVA, may ask for medical information. They will have sought consent as part of the process; the law currently requires to provide information to them if they have assured us that they have your consent, we are not provided with a copy of that consent. We will supply only that information which is relevant and necessary.

Life assurance companies frequently ask for medical reports on prospective clients. These are always accompanied by your signed consent. We will only disclose the relevant medical information according to your consent. You have the right, should you request it, to see reports prepared for insurance companies or employers before they are sent.

Sharing your information without consent

We will normally ask you for your consent, but there are times when we may be required by law to share your information without your consent, for example:

- Where you have become hospitalised and the provider requires medical information such as medication.
- 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;
- Where we encounter infectious diseases that may endanger the safety of others, such as meningitis or measles (but not sensitive information such as HIV/AIDS);
- Where a formal Court Order has been issued;
- Where there is a legal requirement, e.g. if you had committed a Road Traffic Offence.

Use of the practice website

The practice is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using our website, then you can be assured that it will only be used in accordance with this Fair Processing Notice.

You may choose to restrict the collection or use of your personal information in the following ways:

- Information you supply using any electronic form(s) on the practice website will only be used for the purpose(s) stated on the form.
- Your information will not be shared with third parties if you sign up to the practice website.

Right of Access to your Health Information

The GDPR and DPA 2018 allows you to find out what information about you is held on a computer and in manual records. Where information from which you can be identified is held, you have the right to ask to:

- Be informed why, where and how we use your information.
- View this or request copies of the records by making a subject access request – also see below.
- Ask for your information to be corrected if it is inaccurate or incomplete.
- Ask for your information to be deleted or removed where there is no need for us to continue processing it. Note that healthcare information is a special category and cannot be deleted.
- Ask us to restrict the use of your information for non-direct care purposes or for any information we hold that is not part of your healthcare record.
- Ask us to transfer your information to another healthcare organisation
- Object to processing and ask us to stop processing information about you where we are not required to do so by law – although we will first need to explain how this may affect the care you receive.
- Be informed about any automated decision making and profiling if this were to be carried out. And challenge any decisions made without human intervention (automated decision making).
- Withdraw consent where relevant

These rights apply in circumstances where relevant conditions are met.

It is important that you tell us if any of your details such as your name, address or telephone number have changed or if any of your details such as date of birth is incorrect in order for this to be amended. You have a responsibility to inform us of any changes so our records are kept accurate and up to date for you.

Access to personal information

You have a right under the GDPR and DPA 2018 to access/view what information the practice holds about you, and to have it amended or removed should it be factually inaccurate. This is known as 'the right of subject access'. If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding it
- Tell you who it could be disclosed to, and
- Let you have a copy of the information in an intelligible form

We will normally provide you with access via our patient portal, unless you advise us that you do not have access to a computer.

Making a Subject Access Request

If you would like to make a 'subject access request', this can be accepted either verbally, or in writing to the Practice/Service Manager.

- You will need to give us adequate information e.g. full name, address, date of birth, NHS number etc., to enable us to identify you and provide the correct information.
- You will be informed whether a charge will be made for printed copies (a charge will only be made where a request is deemed unfunded or excessive, in line with GDPR Article 12).
- You will receive a response within calendar one month. Where the request is excessive you will be informed if it will take longer for us to respond to your request.

The practice has a leaflet available on making a Subject Access Request, this is available on our website or please ask at reception if you require a copy. On making a request you will be given further information explaining your rights in more detail depending upon which of your rights you are exercising.

Individuals captured by CCTV images

CCTV may be used at premises for security purposes. The practice outsources its CCTV provision to Newcastle City Council which acts as a data processor for the practice. These images are stored in a secured area and are only accessible by authorised staff and are deleted after a designated period as specified in CCTV Code of Practice.

Records Retention - How long do you hold information for?

All records will be retained in line with the Department of Health, The Records Management Code of Practice for Health and Social Care 2016 and will not be held for longer than necessary. This is available on the NHS Digital website at: NHS Records Management Code of Practice. Confidential information is securely destroyed in accordance with this code of practice. This complies with Article 5 of the GDPR Principle 5: 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

Your right to withdraw consent

If you are happy for your data to be extracted and used for the purposes described in this Fair Processing Notice, then you do not need to do anything.

If you do not want your personal data being extracted and used for the purposes described in this Fair Processing Notice, then you need to let us know as soon as possible in writing to the Practice/Service Manager.

Please note that withdrawing your consent from sharing data may, in some circumstances, cause a delay in your receiving care which may result in harm to your health or death if we or other organisations do not have a complete care record.

Your right to opt out

In some instances, you are allowed to request that your confidential information is not used beyond your own care and treatment and to have your objections considered. To support this, patients are

able to register objections with the GP Practice to either prevent their identifiable data being released outside of the GP Practice (known as a Type 1 objection) or to prevent their identifiable data from any health and social care setting being released by NHS Digital (known as a Type 2 objection) where in either case it is for purposes other than direct patient care. If your wishes cannot be followed, you will be told the reasons (including the legal basis) for that decision. There are certain circumstances where a person is unable to opt out, but these are only where the law permits this, such as in adult or children's safeguarding situations.

You have a right in law to refuse or withdraw previously granted consent to the use of your personal information. There are possible consequences of not sharing such as the effect this may have on your care and treatment but these will be explained to you to help with making your decision.
If you wish to exercise your right to opt-out, or to speak to somebody to understand what impact this may have, if any, please contact the Practice using the contact details at the top of this document.

What is the right to know?

The Freedom of Information Act 2000 (FOIA) gives people a general right of access to information held by or on behalf of public authorities, promoting a culture of openness and accountability across the public sector.

What sort of information can I request?

In theory, you can request any information that the practice holds, that does not fall under an exemption. You may not ask for information that is covered by the GDPR/DPA. Your request must be in writing and can be either posted or emailed to the practice.

Concerns About Sharing Your Information

If you have any concerns about how we use or share your information, or you do not wish us to share your information, then please contact the Practice Manager.

Complaints or Queries

We try to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring concerns to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. If you have any queries or concerns about how your information is managed at the practice, please contact the Practice.

Information will be held for the purposes of the complaint with your consent and will be used in the investigation and as part of any necessary enquiries.

If you have any further queries on the uses of your information, please contact:

Liane Cotterill
Senior Governance Manager & Data Protection Officer
North of England Commissioning Support
Teesdale House
Westpoint Road
Thornaby
Stockton on Tees
TS17 6BL

Email: NECSU.IG@nhs.net

If you are not content with the outcome of your confidentiality and data protection concern / complaint raised with the practice you have the right to apply directly to the Information Commissioner's Office for a decision.

Information Commissioner's Office (ICO)

For independent advice about data protection, privacy, data sharing issues and your rights you can contact:

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

Telephone: 0303 123 1113 (local rate) or 01625 545 745 or +44 1625 545 745 (outside UK)
Email: casework@ico.org.uk
Visit the ICO website here https://ico.org.uk/

Changes to Privacy Notice

We keep our Privacy Notice under regular review. The Privacy Notice will be reviewed annually.