

Version	Date Published	Review Status
1.0	May 2018	New document

Changes from the previous version are marked with a line in the margin

BODEY MEDICAL CENTRE **PRACTICE FAIR PROCESSING** **& PRIVACY NOTICE**

Your Information, Your Rights

Being transparent and providing accessible information to patients about how we will use your personal information is a key element of the Data Protection Act 2018 and the EU General Data Protection Regulations (GDPR).

The following notice reminds you of your rights in respect of the above legislation and how your GP Practice will use your information for lawful purposes in order to deliver your care and the effective management of the local NHS system.

This notice reflects how we use information for:

- The management of patient records;
- Communication concerning your clinical, social and supported care;
- Ensuring the quality of your care and the best clinical outcomes are achieved through clinical audit and retrospective review;
- Participation in health and social care research; and
- The management and clinical planning of services to ensure that appropriate care is in place for our patients today and in the future.

Data Controller

As your registered GP practice, we are the data controller for any personal data that we hold about you.

What information do we collect and use?

All personal data must be processed fairly and lawfully, whether is it received directly from you or from a third party in relation to the your care.

We will collect the following types of information from you or about you from a third party (provider organisation) engaged in the delivery of your care:

- ‘Personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified from the data. This includes, but is not limited to name, date of birth, full postcode, address, next of kin and NHS number

And

- ‘Special category / sensitive data’ such as medical history including details of appointments and contact with you, medication, emergency appointments and admissions, clinical notes, treatments,

Version	Date Published	Review Status
1.0	May 2018	New document

Changes from the previous version are marked with a line in the margin

results of investigations, supportive care arrangements, social care status, race, ethnic origin, genetics and sexual orientation.

Your healthcare records contain information about your health and any treatment or care you have received previously (e.g. from an acute hospital, GP surgery, community care provider, mental health care provider, walk-in centre, social services). These records may be electronic, a paper record or a mixture of both. We use a combination of technologies and working practices to ensure that we keep your information secure and confidential.

Why do we collect this information?

The NHS Act 2006 and the Health and Social Care Act 2012 invests statutory functions on GP Practices to promote and provide the health service in England, improve quality of services, reduce inequalities, conduct research, review performance of services and deliver education and training. To do this we will need to process your information in accordance with current data protection legislation to:

- Protect your vital interests;
- Pursue our legitimate interests as a provider of medical care, particularly where the individual is a child or a vulnerable adult;
- Perform tasks in the public's interest;
- Deliver preventative medicine, medical diagnosis, medical research; and
- Manage the health and social care system and services.

How is the information collected?

Your information will be collected either electronically using secure NHS Mail or a secure electronic transferred over an NHS encrypted network connection. In addition physical information will be sent to your practice. This information will be retained within your GP's electronic patient record or within your physical medical records.

Who will we share your information with?

In order to deliver and coordinate your health and social care, we may share information with the following organisations:

- Local GP Practices in order to deliver extended primary care services
 - NHS Organisations including local trusts, hospitals and health boards
 - 111 and Out of Hours Service
 - Medicines Management Team
 - Local Social Services and Community Care services
 - Voluntary Support Organisations commissioned to provide services by Manchester Health Care Commissioners
-

Version	Date Published	Review Status
1.0	May 2018	New document

Changes from the previous version are marked with a line in the margin

Your information will only be shared if it is appropriate for the provision of your care or required to satisfy our statutory function and legal obligations.

Your information will not be transferred outside of the European Union.

Whilst we might share your information with the above organisations, we may also receive information from them to ensure that your medical records are kept up to date and so that your GP can provide the appropriate care.

(In addition we received data from NHS Digital (as directed by the Department of Health) such as the uptake of flu vaccinations and disease prevalence in order to assist us to improve “out of hospital care”.)

How do we maintain the confidentiality of your records?

We are committed to protecting your privacy and will only use information that has been collected lawfully. Every member of staff who works for an NHS organisation has a legal obligation to keep information about you confidential. We maintain our duty of confidentiality by conducting annual training and awareness, ensuring access to personal data is limited to the appropriate staff and information is only shared with organisations and individuals that have a legitimate and legal basis for access.

Information is not held for longer than is necessary. We will hold your information in accordance with the Records Management Code of Practice for Health and Social Care 2016.

Who are our partner software suppliers / businesses?

We use a number of pieces of software and organisations outside of the NHS to facilitate your healthcare and enable our staff to contact you. These are as follows:

Name	Description	Can employees of the organisation access patient information?	GDPR statement
EMIS	Clinical system holds patient demographic and medical information – remote server	The servers and the connection to the practice are encrypted, so EMIS staff are not able to access patient information in this way. EMIS support staff are able to dial in remotely with the consent of our staff for problem solving.	https://supportcentre.emishealth.com/emis-group-and-the-gdpr-general-data-protection-regulation/ (only accessible with a log in so information in Appendix 1)
Oak Telecom	Telephone system – call recording onto a server located within the practice	All the recordings are physically located within the practice. Support staff from oak are able to dial in remotely with the consent of our staff for problem solving.	http://www.oak.co.uk/compliance

Version	Date Published	Review Status
1.0	May 2018	New document

Changes from the previous version are marked with a line in the margin

MJog	SMS and smart messaging system between the practice and patients.	Patient's emis (clinical system) numbers are uploaded to MJog website. The website has an encrypted link to the patient database which is interrogated for the patient's name and mobile number. MJog employees would only have access to this identifiable information when troubleshooting – they will sometimes dial in to an BMC staff member's PC with the consent of the member of staff to fix a problem.	https://www.mjog.com/privacy-policy/ https://www.mjog.com/gdpr-approaches-new-data-protection-legislation/ https://www.mjog.com/data-protection-changes-weeks-away/
Docman	Clinical software which holds patient letters and documents.	Docman support staff can remotely dial in with the consent of our staff for problem solving.	Waiting for information
Docmail	Docmail is an external printing and mailing agency which we use to send larges batches of letters.	Docmail staff can dial in remotely with the consent of our staff for problem solving.	http://www.cfhdocmail.com/tob.html
Greater Manchester CSU	The practice's primary general IT support provider.	Healthcare Computing support staff are able to remotely dial in with the consent of our staff for problem solving.	Waiting for information
Shred-It	Shred paper on which is printed patient or other confidential data	Representative comes to site and collects the four shredding bins full of paper and shreds on site.	Information regarding the service at www.shredit.co.uk
Lexacom	Dictation software which clinical staff use to dictate letters for the secretaries to type.	Lexacom support staff are able to dial in remotely with the consent of our staff for problem solving.	Waiting for information

Version	Date Published	Review Status
1.0	May 2018	New document

Changes from the previous version are marked with a line in the margin

MDU / MPS / MDDUS	Indemnity organisations	We will sometimes send by email or discuss by phone identifiable information when the organisation is supporting a GP in a patient complaint or litigation. Information will be redacted where possible.	https://www.themdu.com/privacy-policy https://www.medicalprotection.org/home/privacy-cookies-policy https://www.mddus.com/mddus-policies/privacy-notice
Broomwell Healthwatch	Broomwell provides software and support for our ECG machine.	Broomwell support staff can remotely dial in with the consent of our staff for problem solving.	www.broomwellhealthwatch.com/privacy-policy
Surgery Website – hosted by Silicon Practice	Provides the platform for online consultations requests / messages to the GP through the surgery website	Silicon Practice support staff are able to dial in remotely with the consent of our staff for problem solving.	Information regarding the service at www.siliconpractice.co.uk/footfall
Great Manchester Shared Services	Manage recall and screening of patients for Diabetic Eye Screening and Cardio Vascular Disease.	The Diabetic Eye Screening Programme is operated by GM shared services (commissioned by NHS England). This supports invitation for eye screening and ongoing care. This data may be shared with any Hospital Eye Services a patient is under the care of to support further treatment and with other healthcare professionals involved in patient care.	www.gmsharedservices.nhs.uk/services
Farsite (through NWEH)	Farsite enables the practice to provide anonymised patient numbers to North West England Health	This enables the practice to work alongside NWEH with research projects and to subsequently help promote research within the NHS	www.nweh.co.uk/how-we-do-it/data-standards

Version	Date Published	Review Status
1.0	May 2018	New document

Changes from the previous version are marked with a line in the margin

Consent and Objections

Do I need to give my consent?

The GDPR sets a high standard for consent. Consent means offering people genuine choice and control over how their data is used. When consent is used properly, it helps you build trust and enhance your reputation. However consent is only one potential lawful basis for processing information. Therefore your GP practice may not need to seek your explicit consent for every instance of processing and sharing your information, on the condition that the processing is carried out in accordance with this notice. Your GP Practice will contact you if they are required to share your information for any other purpose which is not mentioned within this notice. Your consent will be documented within your electronic patient record.

What will happen if I withhold my consent or raise an objection?

You have the right to write to withdraw your consent to any time for any particular instance of processing, provided consent is the legal basis for the processing. Please contact your GP Practice for further information and to raise your objection.

Health Risk Screening / Risk Stratification

Health Risk Screening or Risk Stratification is a process that helps your GP to determine whether you are at risk of an unplanned admission or deterioration in health. By using selected information such as age, gender, NHS number, diagnosis, existing long term condition(s), medication history, patterns of hospital attendances, admissions and periods of access to community care your GP will be able to judge if you are likely to need more support and care from time to time, or if the right services are in place to support the local population's needs.

To summarise Risk Stratification is used in the NHS to:

- Help decide if a patient is at a greater risk of suffering from a particular condition;
- Prevent an emergency admission;
- Identify if a patient needs medical help to prevent a health condition from getting worse; and/or
- Review and amend provision of current health and social care services.

Your GP will use computer based algorithms or calculations to identify their registered patients who are at most risk, with support from the local Commissioning Support Unit (CSU) and/or a third party accredited Risk Stratification provider. The risk stratification contracts are arranged by Manchester Health Care and Commissioning Group (MHCC) in accordance with the current Section 251 Agreement. Neither the CSU nor your local commissioning group will at any time have access to your personal or confidential data. They will only act on behalf of your GP to organise the risk stratification service with appropriate contractual technical and security measures in place.

Your GP will routinely conduct the risk stratification process outside of your GP appointment. This process is conducted electronically and without human intervention. The resulting report is then reviewed by a multidisciplinary team of staff within the Practice. This may result in contact being made with you if alterations to the provision of your care are identified.

Version	Date Published	Review Status
1.0	May 2018	New document

Changes from the previous version are marked with a line in the margin

A Section 251 Agreement is where the Secretary of State for Health and Social Care has granted permission for personal data to be used for the purposes of risk stratification, in acknowledgement that it would overburden the NHS to conduct manual reviews of all patient registers held by individual providers.

As mentioned above, you have the right to object to your information being used in this way. However you should be aware that your objection may have a negative impact on the timely and proactive provision of your direct care. Please contact the Practice Manager to discuss how disclosure of your personal data can be limited.

Sharing of Electronic Patient Records within the NHS

Electronic patient records are kept in most places where you receive healthcare. Our local electronic system (EMIS web) enables your record to be shared with organisations involved in your direct care, such as:

- GP practices
- Community services such as district nurses, rehabilitation services and out of hospital services.
- Child health services that undertake routine treatment or health screening
- Urgent care organisations, minor injury units or out of hours services
- Community hospitals
- Palliative care hospitals
- Care Homes
- Mental Health Trusts
- Hospitals
- Social Care organisations
- Pharmacies

In addition, *NHS* England have implemented the Summary Care Record which contains information including medication you are taking and any bad reactions to medication that you have had in the past.

In most cases, particularly for patients with complex conditions and care arrangements, the shared electronic health record plays a vital role in delivering the best care and a coordinated response, taking into account all aspects of a person's physical and mental health. Many patients are understandably not able to provide a full account of their care, or may not be in a position to do so. The shared record means patients do not have to repeat their medical history at every care setting.

Your record will be automatically setup to be shared with the organisations listed above, however you have the right to ask your GP to disable this function or restrict access to specific elements of your record. This will mean that the information recorded by your GP will not be visible at any other care setting.

You can also reinstate your consent at any time by giving your permission to override your previous dissent.

Version	Date Published	Review Status
1.0	May 2018	New document

Changes from the previous version are marked with a line in the margin

Invoice Validation

If you have received treatment within the NHS, the local Commissioning Support Unit (CSU) may require access to your personal information to determine which Clinical Commissioning Group is responsible for payment for the treatment or procedures you have received. Information such as your name, address, date of treatment and associated treatment code may be passed onto the CSU to enable them to process the bill. These details are held in a secure environment and kept confidential. This information is only used to validate invoices in accordance with the current Section 251 Agreement, and will not be shared for any further commissioning purposes

Your Right of Access to Your Records

You have a right under the General Data Protection Regulations 2018 to request access to view or to obtain copies of what information the surgery holds about you and to have it amended should it be inaccurate. In order to request this, you need to do the following:

- We will initially offer you online access to your Detailed Coded Record - please complete online records access application form (Appendix 2). This contains your electronic medical record, and summarised paper record. It does not contain any letters from the hospitals or other attachments on your record. The advantage of applying for access to this record is that it updates as your medical record updates, so you will always have the most current information.
- If the Detailed Coded Record is not adequate for your needs, please complete the Subject Access Request form (Appendix 3) and we will email you a copy of your medical record (note for information from the hospital you should write direct to them). If you are not able to receive an email containing your medical record, we will print a copy for you. There may be a charge to have a printed copy of the information held about you if the administrative burden of photocopying and printing is excessive.
- We are required to respond to you within 1 calendar month.
- You will need to ensure the request forms are fully completed to give adequate information, so that your identity can be verified and your records located

If you would like access to your GP record please submit your request form to the practice manager:

Bodey Medical Centre
Ladybarn Court
28 Ladybarn Lane
Fallowfield
Manchester
M14 6WP
Email: SMCCG.Bodey@nhs.net

Version	Date Published	Review Status
1.0	May 2018	New document

Changes from the previous version are marked with a line in the margin

Complaints

In the event that you feel your GP Practice has not complied with the current data protection legislation, either in responding to your request or in our general processing of your personal information, you should raise your concerns in the first instance **in writing** to the Practice Manager at:

Bodey Medical Centre
Ladybarn Court
28 Ladybarn Lane
Fallowfield
Manchester
M14 6WP

If you remain dissatisfied with our response you can contact the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF – Enquiry Line: 01625 545700 or online at www.ico.gov.uk

Version	Date Published	Review Status
1.0	May 2018	New document

Changes from the previous version are marked with a line in the margin

APPENDIX 1

EMIS Group and the GDPR (General Data Protection Regulation)

Last updated on [Monday 21 May 2018 news](#)

What is GDPR?

Each member state in the EU operates under the current 1995 data protection regulation and has its own national laws. In the UK, the current Data Protection Act 1998 sets out how your personal information can be used.

The General Data Protection Regulation (GDPR) changes how data can be used and is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen data protection. Companies who hold or process data need to be compliant with the GDPR regulation by 25 May 2018.

What is EMIS Group doing about this?

As an organisation we take issues of information governance and data privacy very seriously and have them at the heart of what we do. Some of what we're doing to ensure compliance with the new regulation is commercially sensitive, however we can confirm we have a project team in place who are currently working on a project plan to ensure that we're compliant.

We are happy to share with you the following high level overview of some of the steps we're taking to address the forthcoming changes in data privacy law:

Raising awareness

We're raising awareness of information governance issues across the group through: the delivery of bespoke training, training modules, use of our internal newsletters and the revised [IG](#) toolkit made available by [NHS Digital](#).

We're revisiting our data breach management policy, including arrangements for compulsory breach notification, so that staff know who to contact should an incident arise.

We will engage with sector specific bodies active in setting standards (e.g. the Information Governance Alliance) so that we are aware of any relevant industry codes of practice.

Product Development

Version	Date Published	Review Status
1.0	May 2018	New document

Changes from the previous version are marked with a line in the margin

We're engaging with our product development teams to identify those elements of the GDPR which we believe may have impact on solution design going forward.

We're revisiting our data protection impact assessment process to ensure that PIA's are undertaken as required.

Review Data Security

We recognise the need to meet the integrity and confidentiality principles under the GDPR. Therefore we're reviewing the below to ensure that they are fit for purpose:

- Data security standards.
- Data breach, storage and destruction policies and management.
- Data security action plan.

Data Protection Officer

We will be appointing a Group DPO with overall responsibility for compliance.

Policy & Contract Review

We're reviewing and updating the below to ensure that they are fit for purpose:

- Data privacy related policies and procedures.
- Data sharing agreements and process.
- Fair processing notices (privacy policies) & website terms.

We will review and revise as appropriate our own terms and conditions and those put forward by our customers so that they reflect the requirements of the new regime.

Version	Date Published	Review Status
1.0	May 2018	New document

Changes from the previous version are marked with a line in the margin

APPENDIX 2



Online Records Access Application Form

Patient Details

Mr Mrs Miss Ms

Surname: _____

First Names: _____

Date Of Birth: _____

Email Address: _____

Current Address: _____

Home Telephone: _____

Mobile Telephone: _____

Please answer the following questions when considering if you would like online access to your medical records:-

1. I am doing this questionnaire for myself **Yes/no**
2. If you answered **no** to question 1, please state your relationship to the patient _____
3. Can you read and understand English? **Yes/no**
4. Have you registered for ordering repeat prescriptions and booking appointments on-line? **Yes/no**
5. Are you happy to use passwords to access your record? **Yes/no**
6. Would you like to feedback what you think of the records access system? **Yes/no**
7. There may be an instance when accessing your medical records online, you may read some information that could be shocking or upsetting. What do you do if this happens and you cannot speak to your doctor/nurse immediately? (please tick all that apply)

- Wait until you see the doctor/nurse for them to explain further**
- Panic and get worked up**
- Look at reputable websites like NHS choices**
- Wait and contact the practice the next working day**
- Contact NHS Direct (111) to get further information**
- Contact GoToDoc, the out of hours service**
- Go to A&E for further help**

8. Would it upset you if you read something somebody else has said about you with regards to your health?

- No**
- Yes – I don't want this information kept in my records**
- Yes – You should not believe what others say**
- Yes – this could destroy our relationship**
- Don't Know**

Version	Date Published	Review Status
1.0	May 2018	New document

Changes from the previous version are marked with a line in the margin

9. Do you feel you understand what Online Records Access means? **Yes/no**

I wish to have access to the following online services (please tick all that apply)

- | | |
|--|--------------------------|
| 1. Requesting repeat prescriptions | <input type="checkbox"/> |
| 2. Booking and cancelling appointments | <input type="checkbox"/> |
| 3. Accessing my medical records summary | <input type="checkbox"/> |
| 4. Accessing my detailed coded medical records | <input type="checkbox"/> |

I wish to access the information I have specified above online and understand and agree with each statement below (tick)

- | | |
|---|--------------------------|
| 1. I have read and understood the information leaflets provided by the practice | <input type="checkbox"/> |
| 2. I have not been coerced or pressured into requesting access to my medical records | <input type="checkbox"/> |
| 3. I will be responsible for the security of the information that I see or download | <input type="checkbox"/> |
| 4. If I choose to share my information with anyone else, this is at my own risk | <input type="checkbox"/> |
| 5. I will contact the practice as soon as possible if I suspect that my account has been accessed by someone without my agreement | <input type="checkbox"/> |
| 6. If I see information in my record that is not about me or is inaccurate, I will contact the practice as soon as possible | <input type="checkbox"/> |
| 7. I agree to use the system responsibly and I am aware that access will be removed as a result of abuse of the system | <input type="checkbox"/> |

Signature of the patient: _____ Date: _____

For office use only

Patient EMIS ID Number : _____

Date Received: _____

Records Checked by (GP): _____

Suitable for online access? **Yes/No** Date: _____

First Method of ID (include ref numbers where applicable) _____

Second Method of ID (include ref numbers where applicable) _____

Date Access Granted & Passwords issued: _____

Signed: _____ Print Name & Position: _____

Version	Date Published	Review Status
1.0	May 2018	New document

Changes from the previous version are marked with a line in the margin

Relationship with individual who's records have been requested					
Address to which a reply should be sent		Postcode: _____ Tel: _____			
4.	Authorisation to release to applicant (to be completed by the patients/clients/staff member if not making their own request)				
<p>I (Print name) _____ hereby authorise the [PRACTICE] to release any personal data they may hold relating to me to the above applicant and to whom I authorise to act on my behalf.</p> <p>Signature of patient/client/staff member : _____ Date: / /</p>					
5.	Declaration				
<p>I declare that information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health record(s) referred to above, under the terms of the Access to Health Records Act (1990) / Data Protection Act.</p> <p>Please select one box below:</p> <p><input type="checkbox"/> I am the patient/client/staff member (data subject).</p> <p><input type="checkbox"/> I have been asked to act on behalf of the data subject and they have completed section 4 -authorisation above.</p> <p><input type="checkbox"/> I am acting on behalf of the data subject who is unable to complete the authorisation section above (Covering letter with further details supplied).</p> <p><input type="checkbox"/> I am the parent/guardian of a data subject under 16 years old who has completed the authorisation section above. (Please include proof such as birth certificate)</p> <p><input type="checkbox"/> I am the parent/guardian of a data subject under 16 years old who is unable to understand the request and who has consented to my making the request on their behalf.</p> <p><input type="checkbox"/> I have been appointed the Guardian for the patient/client, who is over age 16 under a Guardianship order (attached).</p> <p><input type="checkbox"/> I am the deceased patient/client's personal representative and attach confirmation of my appointment.</p> <p><input type="checkbox"/> I have a claim arising from the patient/client's death and wish to access information relevant to my claim (Covering letter with further details to be supplied).</p> <p>Please Note:</p> <ul style="list-style-type: none"> ▪ If you are making an application on the behalf of somebody else we require evidence of your authority to do so i.e. personal authority, court order etc, and It may be necessary to provide evidence of identity (i.e. Driving Licence). ▪ If there is any doubt about the applicant's identity or entitlement, information will not be released until further evidence is provided. You will be informed if this is the case. ▪ We will process your request within one calender month of the original request, providing all forms are completed fully and all supporting documentation is in place. ▪ Under the terms of Section 7 of the Data Protection Act, Information disclosed under a Subject Access Request may have information removed; this is to ensure that the confidentiality is maintained for third parties referred to who have not consented to their information being disclosed. 					
Print Name		Signed (Applicant)		Date	/ /

Please complete and send this document to:

Practice Manager, Bodey Medical Centre, ladybarn Court, 28 Ladybarn Lane, Fallowfield, Manchester, M14 6WP or email to SMCCG.Bodey@nhs.net