Fair Processing Notice under the General Data Protection Regulations (GDPR) 2018 (formerly the Data Protection Act 1998) - How we use your personal information

This fair processing notice explains why the GP practice collects information about you and how that information may be used.

The health care professionals 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, Walk-in clinic, etc.). These records help to provide you with the best possible healthcare.

NHS health records may be electronic, on paper or a mixture of both, and we use a combination of working practices and technology solutions to ensure that your information is kept confidential and secure. Records which this Practice hold about you may include the following information:

- Details about you, such as your address, carer, legal representative, emergency contact details, next of kin
- Any contact the surgery has had with you, such as appointments, telephone, eConsults submitted by you, 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

To ensure you receive the best possible 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 within the GP practice for clinical audit to monitor the quality of the service provided. Some of this information will be held centrally and used for statistical purposes. 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 – if this information needs to be identifiable, the surgery will always gain your explicit consent before releasing the information for this purpose.

Risk Stratification

Risk stratification data tools are increasingly being used in the NHS to help determine a person's risk of suffering a particular condition, preventing an unplanned 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 is then arrived at through an analysis of your anonymised information using software managed by our clinical system provider, and is only provided back to your GP 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.

Medicine 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 pharmacists and Technicians employed by CBC Health Limited. They are bound by the same confidentiality rules as our staff are.

The Hub

The Hub is an organisation which operates across the 2 practices. It offers evening and weekend appointments with a GP . It operates from Prince Consort Road health centre and Blaydon health centre. By booking an appointment with The Hub, patients are explicitly consenting to The Hub staff accessing their medical records to provide medical care. This service is provided by CBC Health Limited.

How do we maintain the confidentiality of your records?

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

- General Data Protection Regulations 2018 (formerly Data Protection Act 1998)
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Health and Social Care Act 2012
- NHS Codes of Confidentiality, Information Security and Records Management
- Information: To Share or Not to Share Review

Every member of staff who works for an NHS organisation has a legal obligation to keep information about you confidential. Any visitor to the premises who will or could be exposed to your identifiable information will sign a confidentiality agreement.

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 (i.e. life or death situations), where the law requires information to be passed on and / or in accordance with the new information sharing principle following Dame Fiona Caldicott's information sharing review (Information to share or not to share) where "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. They should be supported by the policies of their employers, regulators and professional bodies.

Who are our partner organisations?

- NHS Trusts / Foundation Trusts
- GP's
- 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
- Health and Social Care Information Centre (HSCIC)
- Local Authorities
- Education Services
- Fire and Rescue Services
- Police & 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 some cases asked for explicit consent for this happen when this is required. We may also use external companies to process personal information, such as for archiving purposes. These companies are bound by contractual agreements to ensure information is kept confidential and secure.

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)
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

Scan and Collate	Make copies of patient records in response to Subject Access Requests	Representative comes to practice and scans Lloyd George record onto password protected CD which is then sent to patient or Solicitor. No patient data is taken off site.	Nothing is taken off site, so no privacy policy but copy of confidentiality agreement in Appendix 2
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

Access to personal information / Subject Access Requests

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:

- Your request must be made in writing to the GP, this can be made by email or letter (note for information from the hospital you should write direct to them)
- We will initially offer you online access to your Detailed Coded Record. 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 is 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, we will email you a copy of your medical record. If you are not able to receive an email containing your medical record, you 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 20 days
- You will need to give adequate information (for example full name, address, date of birth, NHS number and details of your request) so that your identity can be verified and your records located

Objections / Complaints

Should you have any concerns about how your information is managed at the GP, please contact the Practice Manager/ Operation Manager by letter. If you are still unhappy following a review by the GP practice, you can then complain to the Information Commissioners Office (ICO) www.ico.gov.uk, casework@ico.org.uk, telephone: 0303 123 1113 (local rate) or 01625 545 745.

If you are happy for your data to be extracted and used for the purposes described in this privacy notice then you do not need to do anything. If you have any concerns about how your data is shared then please contact the practice.

Cookies

Our practice website uses cookies to function correctly. You may delete cookies at any time but doing so may result in some parts of the site not working correctly.

Change of Details

It is important that you tell the person treating you if any of your details such as your name or address 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 accurate and up to date for you.

Notification

The General Data Protection Regulations 2018 requires organisations to register a notification with the Information Commissioner to describe the purposes for which they process personal and sensitive information.

This information is publicly available on the Information Commissioners Office website www.ico.org.uk

The practice is registered with the Information Commissioners Office (ICO).

Who is the Data Controller?

The Data Controller, responsible for keeping your information secure and confidential is: Hedge End Medical Centre

If you are still unhappy following a review by the Practice you can then complain to the Information Commissioners Office (ICO). **www.ico.org.uk**, casework@ico.org.uk, telephone: 0303 123 1113 (local rate) or 01625 545 745.

Who is the Data Protection Officer?

The Data Protection officer for the Practice is:

Liane Cotterill

If you would like to contact the Data Protection Officer, please use the following email: NECSU.IG@nhs.net

Or you can write to the DPO at:
Liane Cotterill
Senior Governance Manager & Data Protection Officer
North of England Commissioning Support
Teesdale House
Westpoint Road
Thornaby
Stockton-on-Tees
TS17 6BL

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

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.

APPENDIX 2

SCAN & COLLATE
DOCUMENT MANAGEMENT

Contract Agreement

This is a Contract Agreement between

and

Scan & Collate Ltd
Unit 7
The Innovation Centre
Ebbw Vale
NP23 8XA

This confirms that the above party have employed Scan & Collate Ltd as data processing agents for the purpose of providing secure digital images of their patient's medical records.

All employees of Scan & Collate Ltd who have access to these records have signed a confidentiality agreement and have been DBS (Disclosure and Barring Service) checked and cleared.

Either party may withdraw from this contract by giving 30 days notice of such intent.

Scan and Collate Ltd (S&C) will do the following,

- Check the request letter (if it has been provided), to make sure that the patient name and date of birth on the letter matches that which is on the outside cover of the paper records folder.
- Check if the whole record is required or just from a date range. If from a date range S&C will go through the paper record and when they reach a document which is dated prior to the requested date then they will stop looking and only scan the paper records from that date forward. It is assumed that each record is in chronological order.
- Go through the paper record from front to back and remove all staples and other fixings in order to prepare the record for scanning. The practice should notify S&C of anything which does not require scanning or which needs redaction by using a post it strip or other notification at the top of each affected page to state either do not scan that page or redact something from that page and S&C will carry out those instructions.
- Put each record back in the same order it was prior to scanning and in at least the same condition. (Sometimes we may improve the condition of some paper, i.e. repair torn paper, in order for it to be scanned without causing further damage or to obtain a better quality image.)
- Only process one record at a time to prevent any cross contamination.
- Inform the practice staff of any issues found from conducting the checks in the above points, immediately.
- Keep patient and practice confidentiality at all times, whether heard, seen or read.
- Act on instruction form the practice (Data Owner).

- Supply a “back up” disc of records scanned, in order that the practice may check the data before sending out and quickly and efficiently produce a copy disc should it be required.

Scan and Collate Ltd (S&C) will not,

- Go through the entire record and check each page for any discrepancies (wrong patient for example).
- Take any patient information away with them.
- Make a decision themselves on what if any information should be redacted or omitted.

As the Data Owner, you have ultimate responsibility and in accordance with the statement on the website of the Information Commissioners Office (ICO), it is stated that you “check any records which have required redaction or partial copying” to ensure the process has been completed to your requirements prior to sending outside of the practice.

Quality Standards and Compliance.

Both parties will carry out their obligations under this Agreement with all due care, skill and judgement and will devote all such time, attention and resources as is necessary to ensure that their obligations are discharged to the highest professional standards and in accordance with all applicable regulations.

Both parties will comply with relevant UK law and regulations.

Insurance.

S&C will take out and maintain adequate insurance as may be necessary for the provision of the service including but not limited to public liability with a reputable insurance company.

Confidentiality.

The Practice agrees and warrants at all times during and subsequent to this Agreement to treat as confidential all or any information (in whatever media) regarding the operations, products, finance, marketing, administration, maintenance, research and development, future intentions and policy of S&C or any other information which may be a trade secret or of a confidential nature which the Practice is or becomes aware. Such confidential information will be treated by it with the strictest confidence and secrecy, and further no such information will be disclosed, published or released to any third party or used for the Practice’s own purposes or for any purposes other than those relating to the provision of the service under this agreement without the express written permission of S&C.

S&C agrees and warrants at all times during and subsequent to this agreement to treat as confidential all or any information (in whatever media) regarding the operations, products, finance, marketing, administration, maintenance, research and development, future intentions and policy of the Practice or any other information, including patient information, which may be a trade secret or of a confidential nature which S&C is or becomes aware. Such confidential information will be treated by it with the strictest confidence and secrecy, and further no such information will be disclosed, published or released to any third party or used for S&C’s own purposes or for any purposes other than those relating to the provision of the service under this agreement without the express written permission of the Practice.

The Practice shall provide S&C with the patient records and S&C shall carry out the service in an on site area to be notified by the Practice. S&C will comply in all respects with the Caldicott Principles relating to the processing of patient data and/or as advised by the Practice.

GDPR (General Data Protection Regulations).

S&C keep no personal information or data regarding any patient details. All scanned information is deleted from our computers before leaving the Practice.

S&C only use S&C staff, we do not use temporary or agency staff for this service.

Neither party may assign or transfer all or any part of its rights or obligations under this agreement.

Intellectual Property.
Ownership of intellectual property subsisting in any document (including electronic documents), records, papers, recordings or other material provided by one party to the other is the exclusive property of the party providing it.

If any dispute or difference arises between the parties concerning the construction or performance of this agreement or the rights and liabilities of the parties, the parties will actively, openly and in good faith discuss that dispute or difference with a view to resolving it by mutual agreement.

Signature:	Signature:
Date:	Date:
Name:	Name:
Position:	Position:
Company Name: Scan & Collate Ltd	Practice name: