



UNIVERSITY HEALTH SERVICE

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 University Health Service will use your information for lawful purposes in order to deliver your care and the effective management of the local and national 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;
- Participation in Clinical Research and Clinical Audit 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. We are registered with the Information Commissioners Office – website www.ico.org.uk

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, 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 GP electronic patient record is held securely and confidentially on an electronic system.

When you register with the University Health Service you will complete an online pre-registration questionnaire managed by our clinical system provider EGTON, this information is transferred to us via secure NHS Mail.

Once you are registered with the University Health Service, further information will be collected either electronically using secure NHS Mail or a secure electronic transfer over an NHS encrypted network connection. In addition, physical information will be sent to us from your previous practice if you were formerly registered in the U.K. This information will be retained within your electronic patient record or within your physical medical records. Depending on your personal health situation, we may also store your information elsewhere on our secure NHS network drive as well as other secure locations such as our eating disorder app.

Who will we share your information with?

Your GP electronic patient record is held securely and confidentially on an electronic system, EMIS, managed by EGTON.

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

- Local GP Practices and health providers (e.g. Primary Care Sheffield) in order to deliver extended primary care services in various satellite hubs across Sheffield

- Other NHS services, including secondary care hospitals, both locally and in your home town
- Independent contractors such as pharmacists, dentists and opticians
- Private sector health and social care providers
- 111, ambulance and Out of Hours Service
- Social Services and Community Care services, including health and social care services provided by Sheffield City Council
- Voluntary Support Organisations commissioned to provide services by Sheffield Care Commissioning Group

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, other than in certain circumstances where you request this.

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 receive 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”.

We have a legal duty to share certain information with Public Health England to assist with keeping the population safe. This might include information relating to national screening programmes such as cervical screening and routine vaccination programmes, and will also include information shared in the event of a public health outbreak such as measles or TB.

Some 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. We will share your data with NHS organisations such as NHS Digital and the Clinical Practice Research Datalink, who may pass aggregated information to third party researcher organisations, in order to improve patient services and public health. Individual patient data is not shared, however patients can in some circumstances still opt out of this sharing arrangement. For more information please see the section on ‘Confidentiality’ on our website.

We also outsource some service functions, such as the collection of data for patient surveys and feedback, confidential waste collection and shredding, archiving etc. These companies are bound by contractual agreements to ensure information is kept confidential and secure.

Clinical audit:

Your information may be used for clinical audit to monitor the quality of the service provided. Some of this information may be held centrally and used for statistical purposes. Where we do this we take strict measures to ensure that individual patients cannot be identified e.g. the National Diabetes Audit.

Clinical Research:

Sometimes your information may be requested to be used for research purposes. The Practice may share

anonymised information but will always gain your consent before releasing patient identifiable information for this purpose.

Third party processors

In order to deliver the best possible service, we will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition the practice will use carefully selected third party service providers. When we use a third party service provider to process data on our behalf then we will always have an appropriate agreement in place to ensure that they keep the data secure, that they do not use or share information other than in accordance with our instructions and that they are operating appropriately. Examples of functions that may be carried out by third parties includes:

- Companies that provide IT services & support, including our core clinical systems; systems which manage patient facing services (such as our website and service accessible through the same); data hosting service providers; systems which facilitate appointment bookings or electronic prescription services; etc.
- Payment providers (if for example you were paying for travel vaccinations).

Further details regarding specific third party processors can be supplied on request.

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. There are practice policies in place which staff must adhere to with regards to maintaining patient confidentiality, and a disciplinary process in place should there be significant breaches of these policies.

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 that is not directly or indirectly (e.g. clinical system IT suppliers – please refer to third party processors) involved in your care without your consent unless there are exceptional circumstances, such as life or death situations, or where the law requires it. In certain circumstances we may share patient information without their consent if we believe that refraining from doing so could lead to the harm of the patient and/or to others.

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.

Arrangements between University Health Service (UHS) and The University of Sheffield (TUOS)

Although UHS is a TUOS service, we hold a completely separate record management system to the rest of the University. Other than those employed by UHS, TUOS staff do not have direct access to either our clinical system or any other systems where we hold patient data.

We do not share any information with TUOS without consent from the patient, other than as stated above in the section on “How do we maintain the confidentiality of your data”. If your personal information changes (e.g. name, address, gender etc), in addition to notifying TUOS you must also notify UHS, as this information is not passed to UHS by the University.

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 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.

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 to discuss how disclosure of your personal data can be limited.

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 treatment. This services is provided to practices in Sheffield by Sheffield Care Commissioning Group (CCG).

Sharing of Electronic Patient Records within the NHS

Electronic patient records are kept in most places where you receive healthcare. We will share information with organisations involved in your direct care, such as:

- GP practices
- Community services such as district nurses, rehabilitation services, telehealth 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 some circumstances, some of these organisations will be able to directly access your clinical record, for example, if you are seen at the Extended Access Satellite Hubs within Sheffield. This is because we have enabled our electronic system to allow the organisation access. Clinical and personal details will only be available to any person who is involved with your care, and access to your information is made on a need-to-know basis. Before anyone can view the record there must be a legitimate relationship with the patient and permission from the patient to view the shared record, unless in an emergency situation.

In addition, England has implemented the Summary Care Record which contains information including medication you are taking and any adverse 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.

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

The Data Protection Bill and General Data Protection Regulations allows you to find out what information is held about you, including information held within your medical records, either in electronic or physical format. This is known as the "right of subject access". If you would like to have access to all or part of your records, you can make a request in writing to the organisation that you believe holds your information. This can be your GP, or a provider that is or has delivered your treatment and care. You should however be aware that some details within your health records may be exempt from disclosure, however this will be in the interests of your wellbeing or to protect the identity of a third party. If you would like access to your GP record please submit your request in writing via:

<https://www.sheffield.ac.uk/ssid/health-service/about/viewrecords>

or

The Reception Manager
University Health Service
53 Gell Street
Sheffield
S3 7QP

You may be asked to give adequate information (for example your full name, date of birth, address etc) so we can verify your identity and ensure that we have enough information to locate the records that we hold. We have one month to respond to your request. Generally there will be no charge levied for this service, though in certain circumstances where multiple requests are made we can levy a fee; you will be notified in advance of any fees for this service. Please note that we can only provide the information that we hold at UHS – if you wish to receive copies of hospital records or records which are not held in your GP records, you must contact the service which holds these records.

You can access some of your medical records online. Please contact our reception team for further details on how to do this.

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:

University Health Service
53 Gell Street
Sheffield
S3 7QP

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

Version 1 – 23rd May 2018
Author – B. Graham

Updated January 2020. B. Hallsworth