PRACTICE PRIVACY NOTICE

Last updated: 23rd May 2018 (v1.4)

This is a comprehensive overview on how your personal information is used by our General Practice, the NHS (National Health Service) and our healthcare partner organisations.

Please feel free to ask a member of our staff for separate leaflets on specific data privacy topics such as our Data Privacy guidance for children. Our full contact details are included at the end of this document.

TABLE OF CONTENTS

Contents

HOW DO WE USE YOUR PERSONAL DATA?

How do we use your personal data?

PERSONAL DATA IS ANY INFORMATION THAT RELATES TO AN IDENTIFIED OR IDENTIFIABLE LIVING INDIVIDUAL. DIFFERENT PIECES OF INFORMATION, WHICH COLLECTED TOGETHER CAN LEAD TO THE IDENTIFICATION OF A PARTICULAR PERSON, ALSO CONSTITUTE PERSONAL DATA.

WHAT TYPES OF PERSONAL DATA ARE USED BY OUR GENERAL PRACTICE?

Examples of information we use that constitutes personal data includes:

- Your name, address, telephone numbers, an email address and an identification number (e.g. every patient has a unique NHS ID Number)
- We may hold details on other people such as your carer, legal representative or emergency contacts
- Any contact the surgery has had with you - such as appointments, clinic visits, emergency appointments
- Notes and reports about your health and details about your treatment and care
- Results of investigations such as laboratory tests or x-rays etc.
- Relevant information from other health professionals, relatives or those who care for you
- An online identifier on a website (e.g. website 'cookies' that track) - reflecting changes in internet technology and the way organisations may collect information about individuals.
- CCTV video recordings - captured and stored for the purposes of holding data relating to employee monitoring, staff security and crime prevention.

Our General Practice

OUR GENERAL PRACTICE ENSURES PERSONAL DATA ON OUR PATIENTS AND STAFF IS PROCESSED FAIRLY AND LAWFULLY.

PURPOSE AND LEGAL BASIS FOR PROCESSING YOUR PERSONAL DATA

Our health care professionals who provide you with care maintain records about your health and any treatment or care you have received previously (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.

We want to make sure that you clearly understand why we process your personal information fairly and lawfully for these main reasons:

- the data subject (i.e. the patient) has given consent to the processing of his or her personal data for one or more specific purposes (e.g. to support the delivery of your care);
- processing is necessary for compliance with a legal obligation to which the controller is subject (every General Practice has to record its care provided);
- processing is necessary in order to protect the vital interests of the data subject or of another natural person (i.e. the health and wellbeing of a patient);
- 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 (NHS England and its Clinical Commissioning Groups are tasked by the UK Government to obtain a picture of the health and needs of the local population).

OUR GENERAL PRACTICE

HOW WE PREVENT ILLNESS WITH 'RISK STRATIFICATION' – A TERM WE USE IN THE NHS TO DESCRIBE HOW INFORMATION CAN HELP IMPROVE YOUR HEALTH AND WELLBEING

'Risk stratification' data tools are increasingly being used by the NHS on computer systems to help determine a person's risk of suffering from a particular illness or condition - preventing an unplanned or (re)admission and identifying a need for preventive intervention.

This means that automated-decision making and profiling of patients is performed by the NHS based upon the information about you that is collected from a number of sources including this General Practice and NHS Trusts. A risk score is arrived at through an analysis of your de-identified information (so you cannot be personally identified at this stage) using computer software, and is only provided back to your General Practice as data controller in an identifiable form.

Risk stratification enables your GP to focus on preventing your 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 by contacting our General Practice - contact details are included at the end of this Practice Privacy Notice.

MEDICINES MANAGEMENT – REVIEWING YOU PRESCRIPTIONS

Our General Practice may conduct Medicines Management Reviews of medications prescribed to individual 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 to practices within North Yorkshire through Harrogate and Rural District Clinical Commissioning Group

CCTV CAMERAS – EMPLOYEE MONITORING, STAFF SECURITY & CRIME PREVENTION

Our General Practice may make CCTV video recordings that are captured and stored for the purposes of holding data relating to employee monitoring, staff security and to also identify individuals engaged in criminal activity on our premises. This footage is of sufficient quality to identify individuals and will be made available to the police should they legally request to view it. Our CCTV recordings are stored securely and encrypted wherever possible. Individuals have the right to request a copy of any CCTV footage in which they are in focus and/or clearly identifiable. If the request is valid and permissible we can supply the individual with that footage within 30 days of the validation.

YOUR MEDICAL RECORDS

Your Medical Records

MEDICAL RECORDS CAN BE DEFINED AS A "CHRONOLOGICAL WRITTEN ACCOUNT OF A PATIENT'S EXAMINATION AND TREATMENT THAT INCLUDES THE PATIENT'S MEDICAL HISTORY AND COMPLAINTS, THE PHYSICIAN'S PHYSICAL FINDINGS, THE RESULTS OF DIAGNOSTIC TESTS AND PROCEDURES, MEDICATIONS AND THERAPEUTIC PROCEDURES."

CAN I ASK FOR MY PERSONAL **NHS SUMMARY CARE** MEDICAL RECORDS TO BE DELETED?

There is no absolute 'right to be forgotten' on General Practice computer systems. Patients can ask for their personal data to be erased when there is no compelling reason for its continued processing. Requests by our patients will be assessed on their own merits. We have very good reasons for lawfully processing much of the personal information we hold for the purposes of providing continued patient and community care. In summary patients need to understand how medical records benefit both their own health needs and those of the broader population. Some of the purposes why your personal medical records need to be processed are:

- To ensure you receive the best possible care, your records are used to facilitate the ongoing treatment and emergency care you receive from the NHS – for example in a medical emergency it could be critical for a clinician to know if you suffer allergic reactions to certain medicines.
- Information held about you may be used to help protect the health of the public and to help us manage the NHS.
- NHS England and its Clinical Commissioning Groups are tasked by the UK Government to obtain a picture of the health and needs of the local population.
- Information may be used within our General Practice for clinical audit to monitor the quality of the service we provide.
- 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 – our surgery will always gain your consent before releasing the information for this purpose.

YOUR MEDICAL RECORDS

CAN I OBJECT TO HOW MY INFORMATION IS PROCESSED AND USED ELSEWHERE?

You have the right to control how medical information about you is processed, used, shared, disseminated or sold, for purposes other than your direct medical care - so called **secondary uses** (or purposes). Secondary uses are not about information sharing between healthcare professionals.

Secondary uses include projects involved in risk stratification, "population health management", national clinical audits, research, healthcare planning, commissioning of healthcare services by CCGs (Clinical Commissioning Groups), commercial and even political uses.

You can control your personal confidential information by expressing an objection, or "opt-out" to our surgery. We will then add a special *read-code*, or electronic flag, to your GP record on the computer systems we use. Secondary use objections (classed as either a **Type 1** or **Type 2** opt-outs) will in no way affect how healthcare professionals provide you with direct medical care, or prevent them accessing your medical record if and when appropriate, and with your explicit consent. With a Type 1 or Type 2 opt-out in force, you may still be invited to cervical screening, breast screening, bowel cancer screening, diabetic retinopathy screening, abdominal aortic aneurysm screening, and any other current or future national screening programmes.

Type 1 opt-out

A Type 1 opt-out (sometimes referred to as a **XaZ89 or 9Nu0** opt-out) when present in your GP record, should prevent identifiable information about you being extracted from your GP record, and uploaded to any other organisation for purposes other than your direct care. If you request a Type 1 opt-out then it will prohibit extraction and uploading for all of the following secondary uses:

- Risk stratification schemes
- National clinical audits (such as the National Diabetes Audit)
- The Clinical Practice Research Datalink (CPRD)
- Extraction of de-identified information about you concerning any eMed3 (i.e. fit notes)
- Statement of Fitness to Work reports (i.e. sick notes), uploaded to NHS Digital, and subsequently passed by NHS Digital to the Department of Work and Pensions
- All extractions and uploading of identifiable information about you to NHS Digital, for any secondary purpose (so-called GPES extractions)

Type 2 opt-out

A Type 2 opt-out (sometimes referred to as a **XaaVL or 9Nu4** opt-out) when present in your GP record acts to control information about you as held by NHS Digital (formerly the "HSCIC"). It will not prevent NHS Digital disseminating, sharing, or selling, information about you that is either effectively anonymised (i.e. cannot identify you) or aggregated (i.e. just numbers).

NHS Digital holds information about you obtained from a variety of sources, such as hospital trusts, mental health services, maternity records, community records, collectively known as Hospital Episode Statistics (HES). It also holds some information from your GP record. NHS Digital handles your information with a new tool that people can use to opt out of their confidential patient information being used for reasons other than their individual care and treatment. It will be secure and accessible, and will be available from 25 May 2018 - https://digital.nhs.uk/services/national-data-opt-out-programme

ELECTRONIC PATIENT RECORDS (EPR) SYSTEM

Electronic Patient Records (EPR) system

THIS PRACTICE USES AN EPR (ELECTRONIC PATIENT RECORD) COMPUTER SERVICE SUPPLIED BY AN NHS-APPROVED HEALTH IT SYSTEMS COMPANY WHO ARE LOCATED IN ENGLAND - FOR STORING AND PROCESSING YOUR MEDICAL RECORDS DIGITALLY. YOUR PERSONAL DATA IS REFERRED TO AS A SUMMARY CARE RECORD

This system has been developed to help us treat our patients more effectively and to give healthcare staff quicker and easier access to up-to-date information about your treatment. All practice staff who are directly involved with your care will have some level of access to this system, which will be updated at each point of a patient's care. Your personal EPR is referred to as a **Summary Care Record** - an example of a database that processes your data for primary medical uses only, that is for the provision of direct medical care by healthcare professionals. Your records will include important information about your health, including medical history, medications, current prescriptions, allergies, laboratory test results, radiology images, immunisation status and more. It will also include the required personal information we need for our records, including name, date of birth, address, contact phone number and next of kin contact details.

WHO CAN SEE MY **NHS SUMMARY CARE** RECORD?

Here at the practice we have tight controls in place to ensure that only those directly involved in your care will be allowed access to your Electronic Patient Record and they will only have access to the relevant parts of your Electronic Patient Record that they need in order to do their job. Therefore, anyone who has access to your records:

- Must be directly involved in your care and treatment at the practice
- Will have been assigned a secure access method which uniquely identifies them
- Will only see the information they need to do their job
- Will have their details recorded for every action that is taken on the system

HOW LONG DO YOU KEEP MEDICAL RECORDS FOR?

How long do you keep medical records for?

NHS ENGLAND REQUIRES THAT GP RECORDS SHOULD BE RETAINED UNTIL 10 YEARS AFTER THE PATIENT'S DEATH OR AFTER THE PATIENT HAS PERMANENTLY LEFT THE COUNTRY, UNLESS THEY REMAIN IN THE EUROPEAN UNION. UNLESS THE GP IS NOTIFIED OTHERWISE THE RECORD MUST BE RETAINED FOR 100 YEARS.

CHILDREN AND YOUNG PEOPLE RECORDS

NHS England requires that all types of records for children and young people should be retained until the patient is 25 (or 26 if they are 17 when treatment ends) or eight years after their death, if sooner.

If a child's illness or death could be relevant to an adult condition or have genetic implications for their family, records may be kept for longer.

MATERNITY RECORDS (INCLUDING OBSTETRIC AND MIDWIFERY RECORDS)

NHS England requires that maternity records must be retained for 25 years after the birth of the last child.

MENTAL HEALTH RECORDS

NHS England requires that records of people who have been treated for a mental disorder should be retained for 20 years after the date of last contact between the patient and any healthcare professional employed by the mental health provider, or 8 years after the death of the patient if sooner.

Our Privacy Promise

EVERY MEMBER OF STAFF WHO WORKS FOR AN NHS ORGANISATION HAS A LEGAL OBLIGATION TO KEEP INFORMATION ABOUT YOU CONFIDENTIAL.

WE PROMISE:

- To keep your personal data safe and private.
- To give you ways to manage and review how we process and control your data.
- Not to sell your personal data.
- To handle personal data only in ways that patients would reasonably expect.
- Have a basis in law for collecting and using your data and to not do anything unlawful with it.
- Not use your data in ways that are unfair (e.g. in ways you have not been told about and would not expect; where you have a choice but have not had an opportunity or been told how to exercise it; or where the use has an unjustified adverse effect).
- To be open and transparent about how we intend to use your data and who we will share it with.
- 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 in exceptional circumstances (e.g. life or death situations) or if the law requires it to be passed on.

We also operate in accordance with an information sharing principle following Dame Fiona Caldicott's (The UK Government's appointed National Data Guardian for health and social care) information sharing review; *Information to share or not to share* - "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 are supported by the policies of their employers, regulators and professional bodies.

How the law protects your confidentiality

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

- Data Protection Act 2018 (based on the EU's GDRP – General Data Protection Regulations)
- 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
- Gender Recognition Act 2004
- Freedom of Information Act 2000

OUR LEGAL OBLIGATIONS TO PROTECT YOUR PERSONAL DATA

This General Practice is registered with the UK's Information Commissioners Office (ICO) and complies with the Data Protection Act 1998 and its replacement the Data Protection Act 2018. The law is being updated to reflect a European-wide legal framework that applies from 25 May 2018 onwards and is designed to help improve the protection of personal data of individuals – such as our patients and staff.

This includes protection against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage of your data. It requires that appropriate technical or organisational measures are used – so we have policies, procedures and staff training in place to keep your personal data private.

UK and European law demands that in order for our processing to be fair, the 'data controller' (our General Practice who is in control of processing medical records) has to make certain information available to patients or 'data subjects' by allowing you to make a Subject Access Request - contact details are included at the end of this Practice Privacy Notice should you wish to make a request.

OUR DUTY OF CONFIDENTIALITY

Under common law our General Practice has a legal duty of confidentiality to safeguard the confidential health data of our patients. Because we control patient healthcare records on paper and digitally we are classed as a responsible 'public authority' as well as a 'data controller' by the Information Commissioners Office (ICO) – this is because we decide how, why, what, when and for how long personal data of our patients are processed.

IMPLIED CONSENT

Healthcare providers such as our General Practice generally operate on the basis of implied consent to use patient medical records for the purposes of direct patient care, without breaching confidentiality.

However - we cannot rely on a patient's implied consent to use their confidential personal data for other non-direct patient care related activities and therefore we must justify any processing under another lawful basis, such as explicit patient consent or legal gateway.

WHO ARE OUR PARTNER ORGANISATIONS?

Who are our partner organisations?

We may have to share your information, subject to strict agreements on how it will be used, with the following 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 such as TPP SystmOne and EMIS

Note: in some cases you will be asked for explicit consent for personal data sharing 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.

Subject Access Requests and Data Portability

SUBJECT ACCESS REQUESTS (SAR), RECTIFICATIONS AND ERASURE

You have a right under the Data Protection Act (as amended) to request access to view or to obtain copies of what information our surgery holds about you and to have it amended should it be inaccurate.

In some circumstances you may also request the erasure of your personal data that we hold. In order to request this, you need to do the following:

- Your request must be made in writing to our Data Controller (details below).
- For information from the hospital you should write directly to them.
- Normally there is no charge to have a printed copy of the information we hold about you. However, we may refuse to comply with a request for erasure if it is 'manifestly unfounded or excessive', taking into account whether the request is repetitive in nature. If we consider that your request fits this description, we will justify our decision in writing to you by:
    - requesting a "reasonable fee" in advance to cover our excess administration costs to deal with a very complex request; or
    - refuse to deal with your request - providing a clear justification.
- We are required to respond to you within one month, unless it is a complex request - which we will inform you of. Then we are required to respond to you within two further months.
- 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.

SUBJECT ACCESS REQUESTS AND DATA PORTABILITY

REQUESTING A COPY OR TRANSFER OF YOUR DATA – REFERRED TO AS 'DATA PORTABILITY'

You have the right to data portability. This allows patients to obtain and reuse their personal data they have provided to us for their own purposes across different services – for example, if you migrate to a foreign country you may wish us to transfer or transmit your EPR (Electronic Patient Record) directly to your new healthcare provider who is not part of the NHS - so they can import your medical records into their own IT system.

Patients need to complete our Subject Access Request (SAR) form to request a digital or paper copy of their data or to request an electronic transfer of the data to another data controller.

1. In the first instance we prefer to signpost patients to **NHS Patient Online** – a website where you can view your personal GP record (which includes coded information about allergies, immunisations, diagnoses, medication and test results).
2. In other instances - we can securely email you details of your Summary Care Record via **Encrypted NHS Mail**. This will require your access to a personal email account and a web-browser – so you can setup a free NHS online account to unlock and view your safeguarded medical records that are encrypted by NHS Digital.
3. Alternatively, we can provide your personal medical records as **digital files** – as either text (.txt format) or spreadsheet (.csv format) documents via a secure web transfer service.

In all of the above instances we will need you to verify your identity to ensure that your personal medical records are only released to you - or an appointed person you have authorised us to send your confidential data to.

DATA CONTROLLER

The practice is legally classified as a Data Controller because of the way we process personal data of patients and staff. Our entire organisation is responsible for keeping your information secure and confidential – however our main representative for handling your personal data related questions or Subject Access Requests (SAR) is our Data Protection Officer (DPO).

DATA PROTECTION OFFICER (DPO)

Our Practice Manager is currently the main contact for all personal data queries and Subject Access Requests (SAR) and fulfils the role of our Data Protection Officer until further notice. Contact details are shown in the table below.

WEBSITE COOKIES

Website cookies

Website cookies are small computer files that get sent down to your PC, tablet or mobile phone by websites when you visit them. They stay on your device and get sent back to the website they came from, when you go there again. Cookies store information about your visits to that website, such as your choices and other details. Some of this data does not contain personal details about you or your business, but it is still protected by this Patient Privacy notice. By using our website you agree that we can place these types of cookies on your device, however you can block these cookies using your web browser settings. Our General Practice may use these different types of cookies on our website…

SESSION COOKIES (TEMPORARY ONLY)

Session cookies last only for the duration of your visit and are deleted when you close your browser. These facilitate various tasks such as allowing a website to identify that a user of a particular device is navigating from page to page, supporting website security or basic functionality. Many of the cookies we use are session cookies. For example, they help us to ensure the security of your session, and can also keep you signed in to our website while you move between pages or service your online account. Our session cookies used for security are designed to be very difficult to use except by us when you have an active session. They contain no personal information that can be used to identify an individual.

PERSISTENT COOKIES (LAST FOREVER UNLESS CLEARED BY YOU)

Persistent cookies last after you have closed your browser, and allow a website to remember your actions and preferences. Sometimes persistent cookies are used by websites to provide targeted content based upon the browsing history of the device. We use persistent cookies in a few ways, for example - to remember you have visited our website before and to prevent us showing you a ‘Cookie Information’ banner being shown every time you revisit the website. We also use persistent cookies to allow us to analyse customer visits to our site. These cookies help us to understand how web visitors arrive at and use our site so we can improve our online service.

WEBSITE COOKIES

FIRST AND THIRD PARTY COOKIES

Whether a cookie is a first or third party cookie depends on which website the cookie comes from. First party cookies are those set by or on behalf of the website visited. All other cookies are third party cookies. We use both first party and third party cookies.

PERFORMANCE COOKIES

These cookies collect information about how visitors use a web site, for instance which pages visitors go to most often, and if they get error messages from web pages. These cookies don't collect information that identifies a visitor although they may collect the IP address of the device used to access the site. All information these cookies collect is anonymous and is only used to improve how a website works, the user experience and to optimise our content messages.

FUNCTIONALITY COOKIES

These cookies allow the website to remember choices you make (such as your name in a form). They may also be used to provide services you have requested such as watching a video. The information these cookies collect is anonymised (i.e. it does not contain your name, address etc.) and they do not track your browsing activity across other websites.

TARGETING COOKIES

These cookies collect several pieces of information about your browsing habits. If we use them they are usually placed by advertising networks. They remember that you have visited a website and this information is shared with other organisations such as media publishers. These organisations do this in order to provide you with targeted adverts more relevant to you and your interests. This type of advertising is called online behavioural advertising and place an icon in the top right hand corner of an advert. This icon when clicked, will take you through to the website Your Online Choices where there is more help and guidance for you to Opt-out of this type of advertising. You can block these cookies using your browser settings.

GENERAL PRACTICE CONTACTS FOR PERSONAL DATA

General Practice contacts for personal data

DATA PROTECTION OFFICER (DPO)

Our main contact(s) for all personal data queries and Subject Access Requests (SAR).

CONTACT LIST			
NAME	POSITION	EMAIL	TELEPHONE
	Practice Manager		

GENERAL PRACTICE ADDRESS

<Practice Manager Name>

<General Practice Name>

<Address & Post Code>

Website: _____

COMPLAINTS

Should you have any concerns about how your personal information is managed by our General Practice please contact the Practice Manager at the address shown above. If you are still unhappy following a review by our practice you can then complain directly to the Information Commissioners Office (ICO):

Website: www.ico.org.uk **Email:** casework@ico.org.uk **Tel:** 0303 1231113 (local rate) or 01625 545745

Note: Our Practice has no control over other websites that we may link to. We make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to those websites or the information contained within them.