**Our use of your information**

All practice staff sign a confidentiality agreement. Doctors and nurses are bound by professional duties. Your medical records are held on paper and on computer. The information we hold is protected by legislation including the Data Protection Act. Your medical details may be shared with other medical staff and departments directly involved in your care, including through your Summary Care Record (see <https://digital.nhs.uk/summary-care-records)> or Integrated Care Record (see <https://www.happyhealthylives.uk/our-priorities/digital-transformation/integrated-care-record/privacy-notice/)>; with independent contractors such as dentists, opticians, pharmacists; with private and voluntary sector providers; with Ambulance Trusts; with Integrated Care Boards and Primary Care Networks; with social care services and Local Authorities; with government departments under specific conditions as laid out below; in anonymised form for the purposes of medical research; when a court or the law requires us to do so, for example to prevent infectious diseases from spreading or to check the care being provided to you is safe; for the purposes of safeguarding children.

We will *not* share your medical information with anyone else, including your family, unless you request us to do so. If you would like us to share information with a third party which is not providing you with care (such as an insurance company) we will need your written, signed consent.

You have the right to object to your medical records being shared with those who provide you with care. You have the right to object to your information being used for medical research and to plan health services. You have the right to have any mistakes in your record corrected, but you do not have the right to have correct information removed. You have the right to complain to the Information Commissioner’s Office. Please see the practice privacy notices on this website or speak to a member of staff for more information about your rights.

You can see a summary of your records and individual entries made in the record after January 2023 through the NHS App. To see records before then please complete a Subject Access Request form, available from Reception. You will be provided with a printed copy of your record within one calendar month (within two calendar months for complex requests). We will contact you when the request has been completed. Alternatively, you can ask to see your records in the practice, by submitting a request in writing ensuring you have stated your name, address and contact details. The request will be actioned as soon as possible and within a maximum of 21 days.

**PRIVACY NOTICES HELD AT PRACTICE** Please contact the practice manager to request a copy

CHILDHOOD IMMUNISATIONS DATA COLLECTION

DIRECT CARE- EMERGENCIES

EASY READ LEAFLET

LEGAL REQUIREMENTS

MEDICAL RESEARCH

NATIONAL DIABETES AUDIT COLLECTION

NHS DATA

NHS DIGITAL - DEMOGRAPHICS

NHS DIGITAL - E-REFERRALS

NHS DIGITAL - GP SYSTEMS OF CHOICE

NHS DIGITAL - GP2GP

NHS DIGITAL - REGISTER OF DATA ASSESSTS

NHS DIGITAL - SUMMARY CARE RECORD

NHS- NATIONAL SCREENING PROGRAMMES

PAYMENTS

PUBLIC HEALTH

RISK STRATIFICATIONS

SAFEGUARDING

**Privacy Information for Children**

# What is a privacy notice?

A privacy notice helps your doctor’s surgery tell you how it uses information it has about you, like your name, address, date of birth and all of the notes the doctor or nurse makes about you in your healthcare record.

# Why do we need one?

Your doctor’s surgery needs a privacy notice to make sure it meets the legal requirements which are written in a new document called the General Data Protection Regulation (or GDPR for short).

# What is the GDPR?

What a great question! The GDPR is a new document that helps your doctor’s surgery keep the information about you secure.

# How do you know about our privacy notice?

At your surgery, we have posters in our waiting room and leaflets to give to children and adults and we also have lots of information about privacy on our website, telling you how we use the information we have about you.

# What information do we collect about you?

Don’t worry; we only collect the information we need to help us keep you healthy – such as your name, address, information about your parents or guardians, records of appointments, visits, telephone calls, your health record, treatment and medicines, test results, X-rays and any other information to enable us to care for you.

# How do we use your information?

Another great question! Your information is taken to help us provide your care. But we might need to share this information with other medical teams, such as hospitals, if you need to been seen by a special doctor or sent for an X-ray. Your doctor’s surgery may be asked to help with exciting medical research; but don’t worry, we will always ask you, or your parents or adults with parental responsibility, if it’s okay to share your information.

# How do we keep your information private?

Well, your doctor’s surgery knows that it is very important to protect the information we have about you. We make sure we follow the rules that are written in the GDPR and other important rule books.

# What if I’ve got a long-term medical problem?

If you have a long-term medical problem then we know it is important to make sure your information is shared with other healthcare workers to help them help you, making sure you get the care you need when you need it!

# Don’t want to share?

All of our patients, no matter what their age, can say that they don’t want to share their information. If you’re under 16 this is something which your parents or adults with parental responsibility will have to decide. They can get more information from a member of staff at the surgery, who can also explain what this means to you.

# How do I access my records?

Remember we told you about the GDPR? Well, if you want to see what is written about you, you have a right to access the information we hold about you, but you will need to complete a Subject Access Request (SAR). Your parents or adults with parental responsibility will do this on your behalf if you’re under 16. But if you are over 12, you may be classed as being competent and you may be able to do this yourself.

# What do I do if I have a question?

If you have any questions, ask a member of the surgery team or your parents or adults with parental responsibility. You can:

Contact the Practice Manager. GP practices are data controllers for the data they hold

The Data Protection Officer (DPO) for Dunchurch Surgery is based at Coventry & Rugby ICB.

# What to do if you’re not happy about how we manage your information

We really want to make sure you’re happy, but we understand that sometimes things can go wrong. If you or your parents or adults with parental responsibility are unhappy with any part of our data-processing methods, you can complain. For more information, visit ico.org.uk and select ‘Raising a concern’.

We always make sure the information we give you is up to date. Any updates will be published on our website, in our newsletter and leaflets, and on our posters. This policy will be reviewed annually.

# **DIRECT CARE PRIVACY NOTICE**

This practice may keep data on you relating to who you are, where you live, what you do, your family, possibly your friends, your employers, your habits, your problems and diagnoses, the reasons you seek help, your appointments, where you are seen and when you are seen, who by, referrals to specialists and other healthcare providers, tests carried out here and in other places, investigations and scans, treatments and outcomes of treatments, your treatment history, the observations and opinions of other healthcare workers, within and without the NHS as well as comments and aide memoires reasonably made by healthcare professionals in this practice who are appropriately involved in your health care.

If your health needs require care from others elsewhere outside this practice we will exchange with them whatever information about you that is necessary for them to provide that care. When you make contact with healthcare providers outside the practice but within the NHS it is usual for them to send us information relating to that encounter. We will retain part or all of those reports. Normally we will receive equivalent reports of contacts you have with non-NHS services but this is not always the case.

Your consent to this sharing of data, within the practice and with those others outside the practice is assumed and is allowed by the Law.

People who have access to your information will only normally have access to that which they need to fulfil their roles, for instance admin staff will normally only see your name, address, contact details, appointment history and registration details in order to book appointments; the practice nurses will normally have access to your immunisation, treatment, significant active and important past histories, your allergies and relevant recent contacts; the GP you see or speak to will normally have access to everything in your record.

You have the right to object to our sharing your data in these circumstances but we have an overriding responsibility to do what is in your best interests. Please see below.

|  |  |
| --- | --- |
| 1**) Data Controller**  contact details | Drs Czerniewski, Reynolds, Chesser & Harris. Dunchurch Surgery, Dunsmore Heath, Dunchurch, Rugby, CV22 6AP |
| **2) Data Protection Officer** contact details | If you have any queries please contact the Practice Manager. |
| 3) **Purpose** of the processing | Direct Care is care delivered to the individual alone, most of which is provided in the surgery. After a patient agrees to a referral for direct care elsewhere, such as a referral to a specialist in a hospital, necessary and relevant information about the patient, their circumstances and their problem will need to be shared with the other healthcare workers, such as specialist, therapists, technicians etc. The information that is shared is to enable the other healthcare workers to provide the most appropriate advice, investigations, treatments, therapies and or care. |
| 4) **Lawful basis** for processing | The processing of personal data in the delivery of direct care and for providers’ administrative purposes in this surgery and in support of direct care elsewhere is supported under the following Article 6 and 9 conditions of the GDPR:  *Article 6(1)(e) ‘…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…’.*  *Article 9(2)(h) ‘necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services...”*    We will also recognise your rights established under UK case law collectively known as the “Common Law Duty of Confidentiality”.  Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence, it is also referred to as 'judge-made' or case law. The law is applied by reference to those previous cases, so common law is also said to be based on precedent.  The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.  In practice, this means that all patient information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient. It is irrelevant how old the patient is or what the state of their mental health is; the duty still applies.  Three circumstances making disclosure of confidential information lawful are:   * where the individual to whom the information relates has consented; * where disclosure is in the public interest; and * where there is a legal duty to do so, for example a court order. |
| 5) **Recipient or categories of recipients** of the processed data | The data will be shared with Health and care professionals and support staff in this surgery and at hospitals, diagnostic and treatment centres who contribute to your personal care. |
| 6) **Rights to object** | You have the right to object to some or all the information being processed under Article 21. Please contact the Data Controller or the practice. You should be aware that this is a right to raise an objection, that is not the same as having an absolute right to have your wishes granted in every circumstance |
| 7) **Right to access and correct** | You have the right to access the data that is being shared and have any inaccuracies corrected. There is no right to have accurate medical records deleted except when ordered by a court of Law. |
| 8**) Retention period** | The data will be retained in line with the law and national guidance. <https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016> or speak to the practice. |
| 9) **Right to Complain**. | You have the right to complain to the Information Commissioner’s Office. Use this link <https://ico.org.uk/global/contact-us/> or call 0303 123 1113 (local rate) or 01625 545 745 (national rate). |

**Fair Processing Notice**

Personal data is shared with information governance-compliant organisations to search and identify individuals entitled to health care in the community, recommended by NHSE, but not provided by practices.

**DATA SHARING WITH PATIENTS RISK ASSESSMENT**

**Risk assessment undertaken by Dr Chesser and Emily Hughes 17.11.2022**

The National Accelerated Citizen Access Programme (the National Programme) is bringing in a change around how patients access their GP records through the NHS App or other patient facing applications, which will impact record keeping procedures. This involves the processing of personal and special category data on a large scale, of a sensitive and highly personal nature. In addition, it will include the processing of information relating to vulnerable data subjects, potentially including children where their information forms part of an adult with parental responsibility’s record. The change gives patients access to their record (not limited to coded data) through automated means (access as a default).

Are there any risks to the confidentiality, integrity and availability of personal data? Detail the risk, mitigations and risk score. To produce your risk score, multiply the likelihood score by the severity score. Likelihood (Rare = 1 / Unlikely = 2 / Possible = 3 / Likely = 4 / Almost certain = 5). Severity (Negligeable = 1 / Low = 2 / Moderate = 3 / Significant = 4 / Catastrophic = 5)

**Risk:** Target patient is given access to incorrect record.

**Initial risk score:** 1 & 2

**Measures to reduce risk:** Access to patient data will be controlled by NHS login identification of individual patient. GP practice has a local information incident reporting mechanism in place.

**Risk score after mitigations applied:** 1 & 2

**Risk:** Data is read by an unauthorised party / loss of control over the use of personal data.

**Initial risk score:** 1 & 2

**Measures to reduce risk:** Access to patient data will be controlled by NHS login identification of individual patients. Informing patients, including highlighting that shared devices/logins should be avoided. No change to Proxy Access. GP practice has a local information incident reporting mechanism in place.

**Risk score after mitigations applied:** 1 & 2

**Risk:** Maintaining appropriate data quality, i.e; disclosure exemptions have not been considered (redaction of 3rd party and information causing harm and distress) or applied correctly, test outcomes/diagnosis being shared before GP consultation, lack of documentation of essential data through staff fear of access (leading to change in documentation).

**Initial risk score:** 3 & 3

**Measures to reduce risk:** Completion of DPIA. Review and update of management of process from recording to disclosing through the NHS App and other approved patient facing apps. Staff training including ‘fear of access’ management for staff recording patient health records. See guidelines here: <https://www.gov.uk/government/publications/the-good-practice-guidelines-for-gp-electronic-patient-records-version-4-2011> . GP practice to undertake a sample health records audit. GP systems have functionality to enable users to redact potentially harmful information. Redactions/exemptions are invisible to patients. GP systems have the ability to record a safeguarding flag on the patient medical record, this enables the practices to identify at risk patients. GP practice has a local information incident reporting mechanism in place.

**Risk score after mitigations applied:** 3 & 3

**Risk:** Inappropriate release or over-redaction of information (such as 3rd party information, or that which may cause distress or harm to the patient or others).

**Initial risk score:** 3 & 3

**Measures to reduce risk:** Application of serious harm test to each entry. Completion of DPIA. Review and update of management of process from recording to disclosing through the NHS App and other approved patient facing apps. Staff training including ‘fear of access’ management for staff recording patient health records. See guidelines here: <https://www.gov.uk/government/publications/the-good-practice-guidelines-for-gp-electronic-patient-records-version-4-2011> . GP practice to undertake a sample health records audit. GP systems have functionality to enable users to redact potentially harmful information. Redactions/exemptions are invisible to patients. Guidance on IG portal has further details on when to redact. GP systems have the ability to record a safeguarding flag on the patient medical record, this enables the practices to identify at risk patients. GP practice has a local information incident reporting mechanism in place.

**Risk score after mitigations applied:** 3 & 3

**Risk:** Systems that are integrated with general practice automatically upload information into the patient record without managing patient visibility resulting in inappropriate disclosure.

**Initial risk score:** 3 & 4

**Measures to reduce risk:** Review external digital systems and data flows that automatically upload information onto the GPIT system. Consider types of information that may be automatically uploaded for potential risk and choose to hide from patient view or disable. For types of information that are automatically uploaded, advise patients in advance that information may be displayed before a **Clinician** has had a chance to review and discuss the outcome. For types of information that are hidden, advise patients in advance that they will not be able to see the information.

**Risk score after mitigations applied:** 5 & 4

**Risk:** Record which should be assessed as inappropriate for sharing has not been managed (coded) appropriately.

**Initial risk score:** 2 & 4

**Measures to reduce risk:** Completion of DPIA. Review and update of management of process from recording to disclosing through the NHS App and other approved patient facing apps. Staff training to accommodate change of process. GP practice to undertake a sample health records audit. GP practice has a local information incident reporting mechanism in place.

**Risk score after mitigations applied:** 2 & 4

**Risk:** Lack of staff awareness around patient visibility/use of application, potential implications and how to prevent information from being visible if necessary.

**Initial risk score:** 2 & 4

**Measures to reduce risk:** Staff training to accommodate change of process. GP practice to undertake a sample health records audit.

**Risk score after mitigations applied:** 2 & 4

**Risk:** Risk of short-term increase of patient queries/requests (patients not understanding records e.g. access through Shared Care Record queries etc.)

**Initial risk score:** 5 & 2

**Measures to reduce risk:** Good information materials for patients. Review and update of management of process from recording to disclosing through the NHS App and other approved patient facing apps. Staff training to accommodate change of process.

**Risk score after mitigations applied:** 5 & 2

**Action detail: as above**

**Action approver:** Dr Chesser

**Action owner:** Dr Chesser

**Action due date:** ongoing staff awareness

**Action complete:** ongoing

**Measures approved by:** Dr Chesser 17.11.22

**Residual risks approved by:** Dr Chesser 17.11.22

**DPO advice provided by:** Dr Chesser

Summary of DPO advice: risks assessed as per DPIA

**DPO advice accepted or overruled by:** Dr Chesser

Comments: risks assessed as per DPIA

**Consultation responses reviewed by:** Dr Chesser & Emily Hughes

Comments: risks assessed as per DPIA

**This DPIA will be kept under review by:** Emily Hughes in consultation with Dr Chesser

Next review: November 2023 unless change in processes prior to review date

# **DATA SHARING WITH OUTSIDE ORGANISATIONS PRIVACY NOTICE**

The law requires Dunchurch Surgery to share information from your medical records in certain circumstances. Information is shared so that the NHS or Public Health England can, for example, plan and manage services; check that the care being provided is safe; prevent infectious diseases from spreading.

We will share information with NHS Digital, the Care Quality Commission and local health protection team (or Public Health England) when the law requires us to do so.

We must also share your information if a court of law orders us to do so

**NHS Digital**

NHS Digital is a national body which has legal responsibilities to collect information about health and social care services. It collects information from across the NHS in England and provides reports on how the NHS is performing. These reports help to plan and improve services to patients. This data will not be shared for marketing, advertising, purely commercial or insurance purposes.

NHS Digital will collect most of the structured and coded information in your GP record. This includes data about diagnosis, symptoms, test results, medicines, allergies, vaccinations and appointments, as well as data about your sex, ethnicity and sexual orientation. We also collect data about the members of staff who have treated you. They will not collect your name or full address, written notes (such as details of conversations between you and clinicians), images or documents, data that is more than 10 years old, or data that GPs are not permitted to share by law.

This practice must comply with the law and will send data to NHS Digital, for example, when it is told to do so by the Secretary of State for Health or NHS England under the Health and Social Care Act 2012. More information about NHS Digital and how it uses information can be found at: <https://digital.nhs.uk/home>

NHS Digital sometimes shares names and addresses of patients suspected of committing immigration offences with the Home Office. More information on this can be found here: <https://www.gov.uk/government/publications/information-requests-from-the-home-office-to-nhs-digital>

To opt-out of sharing data with NHS Digital go to <https://www.nhs.uk/using-the-nhs/about-the-nhs/opt-out-of-sharing-your-health-records/>

**Care Quality Commission**

The Care Quality Commission (CQC) is an organisation established in English law by the Health and Social Care act. The CQC is the regulator for English health and social care services to ensure that safe care is provided. They inspect and produce reports on all English general practices in a rolling 5 year program. The law allows CQC to access identifiable patient data as well as requiring this practice to share certain types of data with them in certain circumstances, for instance following a significant safety incident. For more information about the CQC see: [http://www.cqc.org.uk](http://www.cqc.org.uk/)/

The law says that we must report certain serious events to the CQC, for example, when patient safety has been put at risk.

**Public Health**

The law requires us to share data for public health reasons, for example to prevent the spread of infectious diseases or other diseases which threaten the health of the population. We will report the relevant information to local health protection team or Public Health England.

For more information about Public Health England and disease reporting see: <https://www.gov.uk/guidance/notifiable-diseases-and-causative-organisms-how-to-report>

|  |  |
| --- | --- |
| **Data Controller** contact details | Drs Czerniewski, Reynolds, Chesser & Harris. Dunchurch Surgery, Dunsmore Heath, Dunchurch, Rugby,  CV22 6AP |
| **Data Protection Officer** contact details | If you have any queries please contact the Practice Manager. |
| **Purpose** of the processing | Compliance with legal obligations or court order. |
| **Lawful basis** for processing | The following sections of the GDPR mean that we can share information when the law tells us to.  Article 6(1)(c) – ‘processing is necessary for compliance with a legal obligation to which the controller is subject…’  Article 9(2)(h) – ‘processing is necessary for the purpose of preventative…medicine…the provision of health or social care or treatment or the management of health or social care systems and services...’ |
| **Recipient or categories of recipients** of the processed data | The data will be shared with NHS Digital.  The data will be shared with the Care Quality Commission.  The data will be shared with our local health protection team or Public Health England.  The data will be shared with the court if ordered. |
| **Rights to object and the national data opt-out** | There are very limited rights to object when the law requires information to be shared but government policy allows some rights of objection as set out below.  **NHS Digital**  You have the right to object to information being shared with NHS Digital for reasons other than your own direct care.  This is called a ‘Type 1’ objection – you can ask your practice to apply this code to your record.  Please note: The ‘Type 1’ objection, however, will no longer be available after 2020.  This means you will not be able to object to your data being shared with NHS Digital when it is legally required under the Health and Social Care Act 2012.  The national data op-out model provides you with an easy way of opting-out of identifiable data being used for health service planning and research purposes, including when it is shared by NHS Digital for these reasons.  To opt-out or to find out more about your opt-out choices please go to NHS Digital’s website.  NHS Digital sharing with the Home Office  There is no right of objection to NHS Digital sharing names and addresses of patients who are suspected of having committed an immigration offence.    **Public health**  Legally information must be shared under public health legislation. This means that you are unable to object.    **Care Quality Commission**  Data will be shared with the CQC, its officers and staff and members of the inspection teams that visit us from time to time. Legally information must be shared when the Care Quality Commission needs it for their regulatory functions. This means that you are unable to object.    **Court order**  Your information must be shared if it ordered by a court. This means that you are unable to object. |
| **Right to access and correct** | You have the right to access your medical record and have any errors or mistakes corrected. Please speak to a member of staff or look at our ‘subject access request’ policy on this website – [www.dunchurchsurgery.warwickshire.nhs.uk](http://www.dunchurchsurgery.warwickshire.nhs.uk/)    We are not aware of any circumstances in which you will have the right to delete correct information from your medical record; although you are free to obtain your own legal advice if you believe there is no lawful purpose for which we hold the information and contact us if you hold a different view. |
| **Retention period** | GP medical records will be kept in line with the law and national guidance. Information on how long records are kept can be found at: <https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016>  or speak to the practice. |
| **Right to complain** | You have the right to complain to the Information Commissioner’s Office. Use this link <https://ico.org.uk/global/contact-us/> or call the helpline **0303 123 1113** |

**Fair Processing Notice**

Personal data is shared with information governance-compliant organisations to search and identify individuals entitled to health care in the community, recommended by NHSE, but not provided by practices.

# **GENERAL PRACTICE DATA FOR PLANNING & RESEARCH PRIVACY NOTICE**

Please click on link below

[**https://digital.nhs.uk/data-and-information/data-collections-and-data-sets/data-collections/general-practice-data-for-planning-and-research#additional-information-for-gp-practices**](https://digital.nhs.uk/data-and-information/data-collections-and-data-sets/data-collections/general-practice-data-for-planning-and-research#additional-information-for-gp-practices)

**MOBILE PHONE DATA EXCHANGE (AccuRx platform) PRIVACY NOTICE**

|  |  |
| --- | --- |
| Data Controller | Drs Czerniewski, Reynolds, Chesser & Harris.  Dunchurch Surgery, Dunsmore Heath, Dunchurch, CV22 6AP |
| Data Protection Officer | If you have any queries please contact the Practice Manager. |

Step 1: Identify the need for a DPIA

|  |  |
| --- | --- |
| Purpose of the processing | The need for a Data Processing Impact Assessment is the processing, on a large scale, of special categories of data for the use of the AccuRx platform to exchange and store messages pertaining to patients and medical staff. |

|  |
| --- |
| **Describe the nature of the processing:** |
| The GP practice is the data controller, and AccuRx the data processor, as per AccuRx’s [Data Processing Agreement](https://www.accurx.com/data-processing-agreement).  The AccuRx patient-initiated messaging feature allows patients to request and receive support relating to their healthcare concerns. They can make requests to the relevant Healthcare Organisation, at a time convenient to them, for support in relation to their healthcare conditions.  Provision of information by the patient allows the Health or Care Professional dealing with the request to triage requests effectively and make informed decisions about how best to respond - the response could be information or advice, an offer of a consultation, provision of a repeat prescription, test results, or a referral to other services.    This enables the healthcare professional to have an informed view of the patient’s current circumstances before deciding to proceed with either (1) a message follow-up, (2) a phone call follow-up, (3) a video-call follow up or (4) an email.    **User Flow**  ● Patient is directed from their GP website to accuRx site  ● They then get directed to a number of options to submit a request to the practice  ● Before they can submit their request, they must enter: ~dob, ~surname, ~forename, gender, ~postcode, plus contact details including phone number  ● The number the patient puts in will be sent a secure code via SMS, and the patient is asked to enter this code into the webpage before proceeding. If they cannot do this, they can still submit their request. The patient is not given information as to whether the practice 'recognises' them / as to whether their details are correct  ● The practice automatically uses all this information to search for the patient on PDS  ● Practice is able to view all incoming requests, including those which have not been matched to a patient on PDS  ● Any match(es) are displayed to the practice staff as either exact or suggested or unmatched  ● IF the submitted information matches a single patient, AND the contact number submitted is consistent with that on PDS, AND the patient has successfully submitted the secure code sent to this number (i.e. they have passed a two factor authentication process), it's an exact match, and the patient's request will be displayed to the practice as under the patient's information/ record  ● IF the submitted information matches a single patient but the submitted contact number does not match that on PDS, OR if the submitted information and contact number do match to a unique patient, but they have not successfully entered the secure code sent to the contact number listed on PDS, it's a suggested match, and displayed to the practice as such. The practice will be prompted to verify the identity of the patient before proceeding with their request  ● IF the submitted information does not match a single patient (i.e. it matches multiple), OR no patient is found on PDS using the submitted information, it's unmatched, and displayed to the practice as such. The practice will be prompted to verify the identity of the patient before proceeding with their request |

|  |
| --- |
| **Describe the scope of the processing:** |
| The data processed by AccuRx in this case is:  ● Patient data (typically name, identifiers, contact details [mobile], demographic data [DoB; gender], message content (including images), documents/notes, survey responses, metadata)    Patients’ data is generally kept in line with the [Records Management Code of Practice for Health and Social Care 2016](https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016). However, AccuRx would delete the data earlier than suggested by this code if they were informed that the condition of Article 9(3) GDPR and s. 11(1) Data Protection Act 2018 no longer applies.    AccuRx retains the data pertaining to their clients’ and prospects’ medical teams’ members and to non-medical personnel actually or potentially involved in purchasing their services for as long as necessary for the purpose of providing the service, to pursue a sales transaction, or to market their services, subject to the the right to object or not to be subject to direct marketing. Healthcare professionals may contact AccuRx ([support@accurx.com](mailto:support@accurx.com)) to request that AccuRx delete the data held about them.  Data may be shared with sub-processors such as cloud services used for accuRx’s own storage, communications, security, engineering, and similar purposes. AccuRx’s sub-processors operate based on Article 28 GDPR-compliant agreements. AccuRx data is encrypted in transit via HTTPS and encrypted at rest via TDE. AccuRx follow the Microsoft Azure Security and Compliant Blueprint for Platform-as-a-Service web applications, specifically designed for NHS services. See [here](https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services/health-and-social-care-cloud-security-good-practice-guide) and [here](https://docs.microsoft.com/en-gb/azure/storage/common/storage-service-encryption) for further information. |

|  |
| --- |
| **Describe the context of the processing:** |
| The nature of the relationships with the individual is that of health and social care staff providing direct care to patients, who will inevitably sometimes be children and part of other vulnerable groups.    The patient has complete control over how much or how little information they want to provide to the healthcare professional, since it is a form that they are manually inputting. The patient consents by clicking on the link that submits their message to the healthcare professional. Crucially, they have the right to object by simply not submitting a message to the healthcare professional.    Prior to using any AccuRx product and therefore accessing the patient’s response, the healthcare professional must agree to an acceptable use policy.    The nature of the relationship with the individuals participating in patient initiated message is that of a healthcare professional providing direct care to the patient. |

|  |  |
| --- | --- |
| **Describe the purposes of the processing:** | |
| The purpose of using the AccuRx platform is for healthcare staff to communicate with patients (and each other regarding patients) for the provision of healthcare or social care services. | |
| **Compliance and proportionality**? |
| The [lawful bases](https://digital.nhs.uk/binaries/content/assets/legacy/pdf/3/p/igagdprprocessing.pdf) of healthcare staff using the AccuRx platform for communicating with patients is the provision of health care or social care services:  6(1)(e) ‘…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…’.  9(2)(h) ‘…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…’  AccuRx has successfully completed NHS Data Security and Protection Toolkit assurance (under NHS ODS code 8JT17), and both the Cyber Essentials and Cyber Essentials Plus certification. Cyber Essentials is a scheme run by the UK government and the National Centre for Cyber Security to help you know that you can trust your data with a given supplier. AccuRx’s sub-processors operate based on Article 28 GDPR-compliant agreements. AccuRx data is encrypted in transit via HTTPS and [encrypted at rest](https://docs.microsoft.com/en-gb/azure/storage/common/storage-service-encryption) via TDE. AccuRx follow the Microsoft Azure Security and Compliance Blueprint for Platform-as-a-Service web applications, specifically designed for NHS services.  **Patient Triage**    Communications between the patient and healthcare professional are encrypted in transit via HTTPS and responses are [encrypted at rest](https://docs.microsoft.com/en-gb/azure/storage/common/storage-service-encryption) via TDE. Patients are also asked to input their DoB, Surname, Forename, Gender, Postcode plus phone number to verify their identity via an SMS Two-Factor Authentication.  The practice is able to view all incoming requests, including those which have not been matched to a patient on PDS. Any match(es) are displayed to the practice staff as either exact or suggested or unmatched.  IF the submitted information matches a single patient, AND the contact number submitted is consistent with that on PDS, AND the patient has successfully submitted the secure code sent to this number (i.e. they have passed a two factor authentication process), it's an exact match, and the patient's request will be displayed to the practice as under the patient's information/ record.  IF the submitted information matches a single patient but the submitted contact number does not match that on PDS, OR if the submitted information and contact number do match to a unique patient, but they have not successfully entered the secure code sent to the contact number listed on PDS, it's a suggested match, and displayed to the practice as such. The practice will be prompted to verify the identity of the patient before proceeding with their request.    IF the submitted information does not match a single patient (i.e. it matches multiple), OR no patient is found on PDS using the submitted information, it's unmatched, and displayed to the practice as such. The practice will be prompted to verify the identity of the patient before proceeding with their request.     |  |  | | --- | --- | | **Principle** | **Assessment of Compliance** | | **Principle 1 – (2.21 2.23)**  Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –  (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met | Patient consents to take part in the process by completing the form and sending it to the healthcare professional. They can dissent at any point by not messaging the healthcare professional. | | **Principle 2 – (2.2)**  Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. | Personal data is processed under [the lawful basis of the provision of health care or social care services](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/). | | **Principle 3 – ( 3.1)**  Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. | The extent of the patient message purposely has a limit of 200 words per answer in order to ensure the information provided is not excessive and remains relevant to the query. | | **Principle 4 – () 2.12**  Personal data shall be accurate and, where necessary, kept up to date. | The information provided by the patient will give the healthcare professional an up to date view of the patient’s circumstances and this can be added into the patient’s medical record to ensure an accurate and up to date record is maintained. | | **Principle 5 – (2.20)**  Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. | Patient data is kept in line with [**Records Management Code of Practice for Health and Social Care 2016**](https://digital.nhs.uk/binaries/content/assets/legacy/pdf/n/b/records-management-cop-hsc-2016.pdf)**.** These require us to hold records on behalf of GP practices until 10 years after a patient has died. However, we would delete the data earlier than suggested by this code if we are informed that the condition of Article 9(3) GDPR and s.[**11(1) Data Protection Act 2018**](http://www.legislation.gov.uk/ukpga/2018/12/section/11/enacted) no longer applies: “that the circumstances in which the processing of personal data is carried out…[is]by or under the responsibility of a health professional or a social work professional”. | | **Principle 6 – (2.22& 2.23)**  Personal data shall be processed in accordance with the rights of data subjects under this Act. | Patient agrees to take part in the process by submitting the form to the healthcare professional, after acknowledging that the form will be sent to the healthcare professional. They can dissent at any point by not sending the message. | | **Principle 7 – (2.13 2.14 2.16 2.17 2.18)**  Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. | Computer equipment is secure and complies with the NHS standard for encryption. AccuRx has successfully completed NHS Data Security and Protection Toolkit assurance (under NHS ODS code 8JT17), and both the Cyber Essentials and Cyber Essentials Plus certification. AccuRx data is encrypted in transit via HTTPS and encrypted at rest via TDE. | | **Principle 8 – ( 2.15)**  Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. | AccuRx follows the Microsoft Azure Security and Compliant Blueprint for Platform-as-a-Service web applications, specifically designed for NHS services. This means that AccuRx does not store or directly transfer the Personal Data/Special Categories of Personal Data outside of the EEA without a lawful transfer mechanism. However, we draw your attention to the fact that that: a healthcare professional who uses AccuRx to process patient data using a computer outside of the EEA may result in the data being processed outside of the EEA; a patient may be receiving messages whilst outside of the EEA. | |

|  |  |  |  |
| --- | --- | --- | --- |
| Identification and assessment of risks | | | |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
| Access to Personal data by persons other than the data subject | Low | Significant | Low |
| Sensitive data being sent via SMS | Low | Significant | Low |
| Abusive messages are sent to patients by a healthcare professional | Low | Significant | Low |
| The integrity of the computers used (how at risk are they from trojans or viruses) | Low | Minor | Low |

**Patient Initiated Messaging - Risks**

|  |  |  |  |
| --- | --- | --- | --- |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
| A patient sends a message to the GP practice via clinical or admin request pathways and describes red flag symptoms / something that warrants more urgent medical attention. This might not be reviewed by the administrators or clinical team for many days (e.g. over the weekend/ out of hours) | Medium | Significant | Low |
| Any patient can contact any GP practice and submit an admin/ medical request, even if they are not a patient at that practice | Medium | Minor | Low |
| Malicious use of Patient Triage - a malicious actor could submit a large volume of inbound requests and overwhelm a practice's email inbox / AccuRx inbox | Low | Significant | Low |
| Malicious use of Patient Triage - a malicious actor could attempt to contact the GP practice pretending to be another individual | Low | Significant | Low |
| A GP practice could be overwhelmed with more patient initiated requests than they are able to cope with | Medium | Significant | Low |
| For patient initiated messages that are not matched to a patient via PDS, intercepting staff at the practice could not realise that the patient has not been 'authenticated', i.e. that there is no good reason to believe the patient is who they say they are | Medium | Significant | Low |
| Email doesn’t send for whatever reason and patient is waiting for medical help without knowing that their request has not been received | Medium | Significant | Low |
| Following submission of an online consultation, the patient condition deteriorates and doctor can’t get hold of them over phone/video call | Low | Significant | Low |
| Reception encourages someone that calls to use online service. They struggle to use it and abandon, and are too frustrated/scared/worried to call again to get the help they need | Low | Significant | Low |
| Patient enters medical request under clinical request, or vice versa | Low | Minor | Low |
| Patient is unclear when to call 999 /111 | Low | Significant | Low |
| During beta version - user may reply to emails coming into practice email inbox thinking their reply will be sent to the patient. The patient does not receive important clinical information, and the practice does not realise this | Medium | Significant | Low |
| Patient enters medical request under clinical request, or vice versa | Low | Minor | 1 |
| A new patient triage request is not seen in the accuRx Inbox | Low | Significant | 2 |
| A patient triage request is not acted on within a reasonable timeframe | Medium | Significant | 2 |
| Patient or someone acting on behalf of patient attached intimate photos to Patient Triage request | Medium | Significant | 2 |
| A patient is unable to attach an image to their Patient Triage request | Medium | Significant | 2 |
| The image quality is not good enough for **Clinician** to identify issue | Medium | Significant | 2 |
| A malicious user asks patients to send photos via SMS then deletes these from their record | Low | Significant | 2 |
| 1. Stored photos/ documents are accessed by an inappropriate / malevolent user or external hacker  2. Stored photos/ documents are accessed by an inappropriate / malevolent accuRx employee  3. Stored photos/ documents are accessed by an appropriate user, but used inappropriately | Low | Significant | 2 |
| Patients make errors in their medication requests on Patient Triage | Low | Significant | 2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Measures to reduce risk | | | | |
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
| Access to Personal data by persons other than the data subject | Healthcare professionals are authenticated by requiring: NHSmail to register for an account; TPP SystmOne or EMIS Web profiles; and an administrator at their GP practice to approve them. This is to prevent people who do not actually and currently work at the provider organisation from accessing the accuRx system.  Patient demographic data is only pulled from either TPP SystmOne or EMIS Web principal care systems. This ensures that a healthcare professional can only access data of patients registered at their practice.  Any video consultations are not recorded or stored. | Eliminated | Low | Yes |
| Sensitive data being sent via SMS | Healthcare professionals have to agree to an acceptable use policy that includes confirming that the service not be used to communicate SMS messages that are sensitive or clinically urgent messages.    Full **Audit** trails are kept of all healthcare professional activity for clinical safety purposes. | Reduced | Low | Yes |
| Abusive messages are sent to patients by a healthcare professional | AccuRx scans SMSs for abusive content and flags to its Clinical Lead if any are detected.  Full **Audit** trails are kept of all healthcare professional activity for clinical safety purposes. | Reduced | Low | Yes |
| The integrity of the computers used (how at risk are they from trojans or viruses) | Use of devices that comply with NHS standards of encryption. | Reduced | Low | Yes |

**Patient Triage- Measures to reduce risk**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
| A patient sends a message to GP practice via clinical or admin request pathways and describes red flag symptoms / something that warrants more urgent medical attention. This might not be reviewed by the administrators or clinical team for many days (e.g. over the weekend/ out of hours) | Informing the patient at multiple points before submitting their request that 1. their message will not be read out of hours, 2. that their request may not be read for up to 2 working days within normal working hours, 3. that they should seek more urgent medical help if they need a more urgent response, whether from their practice, NHS 111, or 999. Also 4. Screening for 'Red flag' symptoms, and preventing patients submitting a request if they state that they have any of these; 5. prompting patients upon submission of their request to seek more urgent medical attention if their condition deteriorates. | Reduced | Low | Yes |
| Any patient can contact any GP practice and submit an admin/ medical request, even if they are not a patient at that practice | Patients’ queries are flagged to practice staff as 'unmatched' for patients whose submitted information does not match to a patient registered at that practice. The practice is then prompted to confirm the identity of the patient and will have access to the patient’s contact details to let the patient know if they are not registered with that practice. | Reduced | Low | Yes |
| Malicious use of Patient Triage - a malicious actor could submit a large volume of inbound requests and overwhelm a practice's email inbox / accurx inbox | Restricting the number of times someone is allowed to submit the form from a particular location. | Eliminated | Low | Yes |
| Malicious use of Patient Triage - a malicious actor could attempt to contact the GP practice pretending to be another individual | Patients are prompted to submit a phone number upn submission of their request. A 6 digit code is sent via SMS to this phone number, and the patient is prompted to enter this code into the website. If patient requests do not pass this two factor authentication, their request is flagged up to the practice as 'unmatched'. The practice is then prompted to confirm the identity of the patient and will have access to the patient's contact details to let the patient know if they are not registered with that practice. It is possible that some people will have access to the mobile of the person they are trying to imitate and will therefore be able to pass the 2 factor authentication. This is deemed an acceptable level of risk. | Reduced | Low | Yes |
| A GP practice could be overwhelmed with more patient-initiated requests than they are able to cope with | Patients are prompted to call practice if they have not heard from practice after 3 days. Offering analytics of demand will help practices match demand to capacity. | Reduced | Low | Yes |
| For patient-initiated messages that are not matched to a patient via PDS, intercepting staff at the practice could not realise that the patient has not been 'authenticated', i.e. that there is no good reason to believe the patient is who they say they are. | 1. Patients are clearly displayed as 'unmatched' if they are, and 2. GP staff are then prompted to authenticate the patients' identity if needed. Staff are prompted to have a mitigating course of action for these patients. | Reduced | Low | Yes |
| Email doesn’t send for whatever reason and patient is waiting for medical help without knowing that their request has not been received | Stringent internal testing to ensure 100% reliability before product is live. | Reduced | Low | Yes |
| Following submission of an online consultation, the patient’s condition deteriorates and doctor can’t get hold of them over phone/video call | Patient is reminded at multiple times throughout the request process 1. how quickly the practice is likely to respond, 2. that this is not a suitable product for urgent medical requests, and 3. that they should escalate their request to 111 or 999 if they need more emergent care, or if they deteriorate. | Reduced | Low | Yes |
| Reception encourages someone that calls to use online service. They struggle to use it and abandon, and are too frustrated/scared/worried to call again to get the help they need | Practice staff to be encouraged via user guide to only direct patients to complete online requests if they are able to, to call back if they cannot, and for practice staff to fill in online consultation themselves on behalf of the patient where appropriate. | Reduced | Low | Yes |
| Patient enters medical request under clinical request, or vice versa | All requests will be vetted by staff at the practice, and the staff can escalate these as urgent if needed. | Reduced | Low | Yes |
| Patient is unclear when to call 999 /111 | Information to be provided directing patient to NHS website explaining when to call 111/ 999. | Reduced | Low | Yes |
| During beta version - user may reply to emails coming into practice email inbox thinking their reply will be sent to the patient. The patient does not receive important clinical information, and the practice does not realise this. | Emails coming into the practice inbox (for the beta version) have a reminder message at the top not to reply to them. Emails sent to the sending (accurx.nhs.net) email account will also get an automatic reply, advising that the patient will not receive their sent email. | Reduced | Low | Yes |
| Patient enters medical request under clinical request, or vice versa | All requests will be vetted by staff at the practice, and the staff can escalate these as urgent if needed | Reduced | Low | Yes |
| A new patient triage request is not seen in the accuRx Inbox | - Users are notified on new patient triage requests via a notification banner and red dot containing the number of unread messages  - When a user is viewing the inbox, there are additional red dots with numbers inside to indicate unread messages in each folder  - Patient Triage requests are visible to all users to ensure messages are not stuck in someone's inbox if they are out of practice on the day | Reduced | Low | Yes |
| A patient triage request is not acted on within a reasonable timeframe | - Although assignment helps show the practice who is responsible for acting on a patient triage request, all patient triage requests are visible to non-asignees. This was an intentional design decision to ensure that the practice has an overview of all patient triage requests and can monitor any that have not been acted on in a timely manner  - The webpage where the patient enters their symptoms has a section where the patient is informed not to use the form for medical emergencies and requests may not be seen for 2 working days. Patients need to click to confirm they do not have symptoms constituting a medical emergency.  - There is an urgent flag that a user can apply to a patient triage request. This turns the patient triage request selection red, adds a red flag icon and indicates to other users that the request is of higher urgency. | Reduced | Low | Yes |
| Patient or someone acting on behalf of patient attached intimate photos to Patient Triage request | Patients are prompted not to attach any intimate images and have to actively consent that they have not done so before submission. | Reduced | Low | Yes |
| A patient is unable to attach an image to their Patient Triage request | - A patient can discuss the issue by calling the practice  - A patient can contact accuRx support, for technical assistance  - Practice staff can respond to the Patient Triage request, asking for a photo and sending an SMS to enable this pro | Reduced | Low | Yes |
| The image quality is not good enough for **Clinician** to identify issue | - A user can see the patient face to face  - A user can contact the patient to retake the photo with advice  - A user can send an image in via email (not available at all practices)  - Helper text is displayed to the patient to guide them to take a better photo, advising them to (1) use adequate lighting, (2) make sure image is in focus and (3) uses an object for scale | Reduced | Low | Yes |
| A malicious user asks patients to send photos via SMS then deletes these from their record | - Although a user can delete an image from the patient's EMIS record, they are unable to delete it from the accuRx server. This allows an **Audit** trail of images | Reduced | Low | Yes |
| 1. Stored photos/ documents are accessed by an inappropriate / malevolent user or external hacker  2. Stored photos/ documents are accessed by an inappropriate / malevolent accuRx employee  3. Stored photos/ documents are accessed by an appropriate user, but used inappropriately | (1), (2) We follow recommended best practice for storing documents and photos, they are encrypted at rest, and no one has direct access to the files; rather - they are only accessible on an individual basis by authenticated practice users through secure channels. (3) Photos can be 'soft' deleted so that users cannot access them going forward. We have logs of photos accessed for >= the past 12 months, and these can be used to inform an **Audit** trail if needed. We encourage submissions to be saved to the patient's record, and provide best practice guidance to users around processing photos. | Reduced | Low | Yes |
| Patients make errors in their medication requests on Patient Triage | Staff are trained to check medication requests from patients and should be alert to possible errors. Practices are able to customise repeat prescription requests to direct patients to more secure prescription services already offered by the practice, such as Patient Access. | Reduced | Low | Yes |

**Fair Processing Notice**

Personal data is shared with information governance-compliant organisations to search and identify individuals entitled to health care in the community, recommended by NHSE, but not provided by practices.

**Targeted Lung Health Check Privacy Policy Statement**

The Targeted Lung Health Checks (TLHC) programme is a new and ground-breaking flagship programme of work which forms part of the NHS long term plan. This is currently a pilot programme with a capped population in Coventry and Rugby and is currently being offered to select GP practices in the area.

The programme will directly invite people aged over 55 years old but less than 75 years old that have ever smoked to a FREE lung check with one of the NHS Lung Health Check nurses. Following the lung health check those assessed as high risk will be offered a low dose CT scan.

The Practice shares your lung health related data with the Lung Health Check programme operated by University Hospitals Coventry and Warwickshire NHS Trust and InHealth (commissioned by NHS England).

This supports your invitation for a lung health check appointment (if you are eligible) and possible CT scan by the Lung Health Check team. This data may be shared with University Hospitals Coventry and Warwickshire NHS Trust to support further treatment and with other healthcare professionals involved in your care. Further details about how this project and the NHS use your information can be found here and on NHS England’s website.

For further information about the TLHC programme, please see our website (<https://www.happyhealthylives.uk/lunghealthchecks/>) or alternatively, contact the TLHC team directly by emailing [UHCW.LungHealthChecksCoventry@nhs.net](mailto:UHCW.LungHealthChecksCoventry@nhs.net).