PRIVACY NOTICE
Protecting your Confidentiality

Your information - what you need to know. This privacy notice explains why we collect information about you, how that information may be used and how we keep it safe and confidential.

Why we collect information about you. Health care professionals who provide you with care are required by law to maintain records about your health and any treatment or care you have received within any NHS organisation. These records help to provide you with the best possible healthcare. We collect and hold data for the sole purpose of providing healthcare services to our patients. In carrying out this role we may collect information about you which help us respond to your queries or secure specialist services. We may keep your information in written form and/or in digital form. The records may include basic details about you, such as your name and address. They may also contain more sensitive information about your health and also information such as outcomes of needs assessments.

Details we collect about you. The health care professionals who provide you with care maintain records about your health and any treatment or care you have received previously (eg. NHS Hospital Trust, GP Surgery, Walk-in centre, etc.). These records help to provide you with the best possible healthcare.

Records which this GP Practice may hold about you may include the following:

- *Details about you, such as your address and next of kin*
- *Any contact the surgery has had with you, such as appointments, clinic visits, emergency appointments, etc.*
- *Notes and reports about your health*
- *Details about your treatment and care*
- *Results of investigations, such as laboratory tests, x-rays, etc.*
- *Relevant information from other health professionals, relatives or those who care for you*

Your medical record is held in a computer system called SystmOne. This system is provided to us under a National contract with NHS England. Your data is held and managed in secure data centres. Your paper records are stored at a secure facility by Notespace/Oasis Group

How we keep your information confidential and safe. Everyone working for the NHS is subject to the Common Law Duty of Confidence. Information provided in confidence will only be used for the purposes advised with consent given by the patient, unless there are other circumstances covered by the law. The NHS Digital Code of Practice on Confidential Information applies to all our staff and they are required to protect your information, inform you of how your information will be used, and allow you to decide if and how your information can be shared. All our staff are expected to make sure information is kept confidential and receive annual training on how to do this.

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. Your records are backed up securely in line with NHS standard procedures. We ensure that the information we hold is kept in secure locations, is protected by appropriate security and access is restricted to authorised personnel. We also make sure external data processors that support us are legally and contractually bound to operate and prove security arrangements are in place where data that could or does identify a person are processed. We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- *Data Protection Act 1998*
- *General Data Protection Regulation 2018*
- *Human Rights Act*
- *Common Law Duty of Confidentiality*
- *NHS Codes of Confidentiality and Information Security*
- *Health and Social Care Act 2015*

We maintain our duty of confidentiality to you at all times. We will only ever use or pass on information about you if others involved in your care have a genuine need for it. We will not disclose your information to any third party without your permission unless there are exceptional circumstances or where the law requires information to be passed on; for example

- There is a serious risk of harm or abuse to you or other people;
- Safeguarding matters and investigations
- Serious crime, such as assault, is being investigated or where it could be prevented;
- Notification of new births;
- In cases of infectious diseases encouters that may endanger the safety of others, such as meningitis or measles (but not HIV/AIDS);
- A formal court order has been issued;
- There is a legal requirement, for example if you had committed a Road Traffic Offence.

We are required under UK law to keep your information and data for the full retention periods as specified by the NHS Records management code of practice for health and social care and national archives requirements. More information on records retention can be found online at https://transform.england.nhs.uk/information-governance/guidance/records-management-code

How we use your information. We need your personal, sensitive and confidential data in order to provide you with healthcare services as a General Practice, under the General Data Protection Regulation we will be lawfully using your information in accordance with: -

Article 6, e) 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;"

Article 9, (h) processing is necessary for the purposes of preventive 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

This Privacy Notice applies to the personal data of our patients and the data you have given us about your carers/family members.

We use your personal and healthcare information in the following ways:

- when we need to speak to, or contact other doctors, consultants, nurses or any other medical/healthcare professional or organisation during the course of your diagnosis or treatment or on going healthcare;
- when we are required by law to hand over your information to any other organisation, such as the police, by court order, solicitors, or immigration enforcement.
- In a de-identified form to support planning of health services and to improve health outcomes for our population

We will never pass on your personal information to anyone else who does not need it, or has no right to it, unless you give us consent to do so.

Legal justification for collecting and using your information. The law says we need a legal basis to handle your personal and healthcare information.

- **Contract:** We have a contract with NHS England to deliver healthcare services to you. This contract provides that we are under a legal obligation to ensure that we deliver medical and healthcare services to the public.

- **Consent:** Sometimes we also rely on the fact that you give us consent to use your personal and healthcare information so that we can take care of your healthcare needs.
- **Necessary care:** Providing you with the appropriate healthcare, where necessary. The Law refers to this as 'protecting your vital interests' where you may be in a position not to be able to consent.
- **Law:** Sometimes the law obliges us to provide your information to an organisation (see above).

You have the right to withdraw consent at any time.

Special categories. The law states that personal information about your health falls into a special category of information because it is very sensitive. Reasons that may entitle us to use and process your information may be as follows:

- **Public Interest:** Where we may need to handle your personal information when it is considered to be in the public interest. For example, when there is an outbreak of a specific disease and we need to contact you for treatment, or we need to pass your information to relevant organisations to ensure you receive advice and/or treatment
- **Consent:** When you have given us consent
- **Vital Interest:** If you are incapable of giving consent, and we have to use your information to protect your vital interests (eg if you have had an accident and you need emergency treatment)
- **Defending a claim:** If we need your information to defend a legal claim against us by you, or by another party
- **Providing you with medical care:** Where we need your information to provide you with medical and healthcare services

Under the powers of the Health and Social Care Act 2015, NHS Digital can request personal confidential data from GP Practices without seeking patient consent. Improvements in information technology are also making it possible for us to share data with other healthcare providers with the objective of providing you with better care. You may choose to withdraw your consent to personal data being used in this way.

When we are about to participate in a new data-sharing project we will make patients aware by displaying notices in the Practice and on our website as far as practicable in advance of the scheme start date. Instructions will be provided to explain what you have to do to 'opt-out' of each new scheme. You can object to your personal information being shared with other health care providers but if this limits the treatment that you can receive then the clinician may have to override this in the best interests of patient safety and care.

To ensure you receive the best possible care, your records are used to facilitate the care you receive. Information held about you may be used to help protect the health of the public and to help us manage the NHS. We will be bound to follow any directives from Government that may affect this, for example, the Coronavirus Act.

GP Connect System and Data Sharing. Acorn surgery has signed the National Data Sharing Arrangement (NDSA) for GP connect. GP Connect helps clinicians gain access to GP patient records during interactions away from a patient's registered practice and makes their medical information available to appropriate health and social care professionals when and where they need it, to support the patient's direct care.

From a privacy, confidentiality and data protection perspective, GP Connect provides a method of secure information transfer and reduces the need to use less secure or less efficient methods of transferring information, such as email or telephone.

GP Connect - key points**.**

- GP Connect can only be used for direct care purposes.
- Individuals can opt out of their GP patient record being shared via GP Connect by contacting their GP practice.
- Access to GP Connect is governed by role-based access control (RBAC) and organisational controls; only people who need to see the GP patient record for a patient's direct care should be able to see it
- All systems that allow the use of GP Connect must undergo a robust compliance process and the organisations involved must sign a connection agreement holding them to high standards of information security.

GP Connect products can help health and social care professionals share, view or act on information that could be required for a patient's direct care, but they would otherwise have difficulty accessing easily (for example if they are using different IT systems).

Organisations can have access to relevant information in GP patient records to provide direct care to patients only.

Type of organisations that use GP Connect Examples of organisations that may wish to use GP connect to view GP patient records include:

- GP surgeries that patients are not registered at - for example, if they need to see a doctor when they are away from home
- Secondary care (hospitals) if they need to attend A&E or are having an operation
- GP hubs/primary care networks (PCNs)/integrated care systems (ICSs), partnerships between healthcare providers and local authorities
- Local 'shared care' record systems
- Ambulance trusts, so paramedics can view GP patient records in an emergency
- Healthcare professionals such as community services
- Acute and emergency care service providers
- NHS 111
- Pharmacies
- Optometrists
- Dentistry
  - Mental health trusts
  - Hospices
  - Adult and children's social care
  - Residential and nursing homes

All access to your GP patient record is stored within an audit trail at your GP practice and within the organisation that information has been shared with.

Confidentiality. Confidentiality and trust are essential to the relationship between GPs and their patients. The information a patient provides to their GP is confidential, and they can expect that any information that is shared for their direct care will remain confidential.

GP Connect relies on 'implied consent'.

Explicit consent is not required when information is shared for a direct care purpose. If a patient does not want their information to be shared using GP Connect, they can opt out.

The NDSA and its terms and conditions stipulate that any information received or accessed about a patient for direct care purposes must remain confidential.

In addition to the NDSA, health and social care professionals are also subject to their own professional codes of confidentiality and are aware that any information received via GP Connect is provided in confidence, which must be respected.

Organisations using GP Connect are notified of their duty as 'controllers' to be fair and transparent about their processing of their patients' information and to ensure that their transparency notices are fully updated with how they may be using GP Connect functionality.

NHS England helps support the mitigation of information sharing risks by ensuring that:

- NHS England audit data access is subject to two-factor authentication and role- based access controls - only certain assured users can have access to the full audit logs
- a completed Supplier Conformance Assessment List (SCAL) which covers service and capability specific compliance requirements and controls of the consumer system is in place

It is the responsibility of organisations using GP Connect to ensure that they comply with the NDSA, and their statutory and legal obligations regarding data protection and confidentiality.

Opting out of GP Connect If you do not wish for your information to be shared using GP Connect, you can opt out by contacting the Practice.

OpenSAFELY

NHS England has been directed by the government to establish and operate the OpenSAFELY COVID-19 Service and the OpenSAFELY Data Analytics Service.

These services provide a secure environment that supports research, clinical audit, service evaluation and health surveillance for COVID-19 and other purposes.

Each GP practice remains the controller of its own GP patient data but is required to let approved users run queries on pseudonymised patient data. This means identifiers are removed and replaced with a pseudonym.

Only approved users are allowed to run these queries, and they will not be able to access information that directly or indirectly identifies individuals.

Patients who do not wish for their data to be used as part of this process can register a type 1 opt out with their GP. Here you can find additional information about OpenSAFELY."

National Screening Campaigns.

GP Surgery Privacy Notice for the Targeted Lung Health Check (TLHC) Programme As part of the NHS's Targeted Lung Health Check (TLHC) Programme, our GP surgery is supporting efforts to detect lung disease, including lung cancer, at an early stage in patients at higher risk. Your data will be used to identify and invite the eligible cohort of patients to receive a telephone triage appointment; if high risk for possibly developing of lung cancer, to invite for a physical nurse-led lung health check consultation, followed by a low-dose CT scan (if appropriate).

To assess your eligibility and facilitate the TLHC Programme, we may share and process:

- **Personal details** (e.g., name, date of birth, NHS number, contact details)
- **Health information** (e.g., medical history, smoking status, scan results, and other relevant health data)
- **Demographic data** (e.g., age, gender, ethnicity) for service monitoring and research purposes

Your personal data will be used to:

- Identify eligible patients for the TLHC Programme
- Invite you to participate in a lung health check
- Conduct assessments and necessary follow-ups
- Communicate results and arrange further investigations if needed
- Monitor and improve the effectiveness of the TLHC Programme through anonymised data analysis
- Ensure quality assurance and service improvements

Legal Basis for Processing Your Data We process your personal data under the following legal bases:

- **Public task**: The TLHC Programme is part of the NHS's responsibility to provide preventive healthcare.
- **Legal obligation**: We comply with health and safety laws and other legal requirements.
- **Consent**: In some cases, we may seek your explicit consent for processing specific information.

Data Sharing and Confidentiality Your data may be shared with:

- NHS organisations and approved partners involved in delivering the TLHC Programme
- Healthcare professionals, including your GP and specialist teams, where necessary for your care
- Research and statistical bodies (in anonymised form where applicable)

General Practice Solutions (GPS) We have a large volume of patient correspondence (such as hospital letters, referrals, and test results). GPS provides specialist staff who review and code these documents directly into your electronic health record (SystmOne). This helps us keep your medical record accurate, up to date, and ensures important clinical information is not missed.

What information is shared?

GPS staff access patient letters and related information necessary for coding and filing into your record. This may include your name, NHS number, date of birth, diagnoses, treatments, safeguarding information, and correspondence from other providers.

How is your data protected?

- GPS staff are bound by confidentiality agreements and the same data protection laws as NHS staff.
- They access records only via secure NHS-approved systems.
- All activity is logged and audited.
- Sensitive information, such as safeguarding concerns, is managed under strict rules and visibility settings.

Who is responsible for your data?

Acorn Surgery remains the Data Controller for your medical records. GPS acts as a Data Processor, working only under our instruction. They cannot use your data for any other purpose.

Your rights

You have the same rights under UK GDPR as explained in our main privacy notice, including the right to access your records, request corrections, and raise concerns. If you have any questions about this processing, please contact our Data Protection Officer.

Transcription of Consultations using Heidi At our GP practice, we prioritise the privacy and confidentiality of your personal health information. We utilise Heidi AI, an advanced artificial intelligence assistant, to assist in clinical documentation during your consultations. Please be assured of the following:

No Information Storage Heidi AI does not store any of your personal health information. All data processed by Heidi AI is deleted immediately after the consultation and successful transfer of information to your medical record. Encryption and regular audits ensure security and compliance.

Data Security Your information is securely handled during the consultation process, ensuring that it remains confidential and protected at all times.

Purpose of Use The sole purpose of using Heidi AI is to enhance the accuracy and efficiency of clinical documentation, thereby improving the quality of care you receive.

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 treatments. The reviews are carried out by the ICBs Medicines Management Team under a Data Processing contract with the Practice.

Requests for medical reports. Should a company require health data to assess a claim.

In most cases, the requester will provide us with a signed consent from you to release information held in your health record. It is the responsibility of the data controller to verify all requests from data subjects using reasonable measures. The Practice will contact you to explain the extent of disclosure sought by the third

party and to obtain your consent to share the data. You will be then given the opportunity to review the information within the record or report and decide whether you content to share the information.

Clinical Audit. 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 and National Obesity Audit. Further information relating to both the mentioned audits can be found below. National Diabetes Audit (England): Transparency Notice - NHS Digital https://digital.nhs.uk/data-and-information/clinical-audits-and-registries/national-obesity-audit/transparency-notice

Clinical Research. Sometimes your information may be requested to be used for research purposes your consent will always be obtained before releasing the information for this purpose.
We share information from medical records;

- to support medical research when the law allows us to do so, for example to learn more about why people get ill and what treatments might work best;
- we will also use your medical records to carry out research within the practice.

This is important because:

- the use of information from GP medical records is very useful in developing new treatments and medicines;
- medical researchers use information from medical records to help answer important questions about illnesses and disease so that improvements can be made to the care and treatment patients receive.
- We share information with the following medical research organisations with your explicit consent or when the law allows:
    - Clinical Practice Research Datalink. For more information https://www.cprd.com/data-protection-and-processing-notice
    - Royal College of General Practitioners (RCGP) Research Surveillance Centre Data who collect coded medical record data as part of the National surveillance system for influenza and other infectious diseases, including new or emerging infections. The data is also used to assess vaccine effectiveness and for other research purposes. For more information: http://www.rcgp.org.uk/clinical-and-research/our-programmes/research-and-surveillance-centre.aspx ,
    - National Institute for Health Research, Care Research Network (CRN), CRN Eastern.
- You have the right to object to your identifiable information being used or shared for medical research purposes.

For more information on how your data may be used in research, click here

National Registries. National Registries (such as the Learning Disabilities Register) have statutory permission under Section 251 of the NHS Act 2006, to collect and hold service user identifiable information without the need to seek informed consent from each individual service user.

Cabinet Office. The use of data by the Cabinet Office for data matching is carried out with statutory authority under Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under the Data Protection Act 1998. Data matching by the Cabinet Office is subject to a Code of Practice. Information on the Cabinet Office's legal powers and reasons why it matches particular information. https://www.gov.uk/government/publications/code-of-data-matching-practice-for-nationalfraud-initiative

Risk Stratification. Risk stratification is a process for identifying and managing patients who are most likely to need hospital or other healthcare services. Risk stratification tools used in the NHS help determine a person's risk of suffering a particular condition and enable us to focus on preventing ill health and not just the treatment of sickness. Information about you is collected from a number of sources including NHS Trusts and from this GP Practice. A risk score is then arrived at through an analysis of your de-identified information using software managed by the Commissioning Support Unit and provided back to this Practice. If necessary we may be able to offer you additional services. Risk stratification is commissioned by the NHS Integrated Commissioning Board (ICB) or its successor organisation.

Section 251 of the NHS Act 2006 provides a statutory legal basis to process data for risk stratification purposes. Further information about risk stratification is available from: www.england.nhs.uk/ourwork/tsd/ig/risk-stratification/.

If you do not wish information about you to be included in the risk stratification programme, please let us know. We can add a code to your records that will stop your information from being used for this purpose.

Individual Funding Request. An 'Individual Funding Request' is a request made on your behalf, with your consent, by a clinician, for funding of specialised healthcare which falls outside the range of services and treatments that CCG has agreed to commission for the local population.

An Individual Funding Request is taken under consideration when a case can be set out by a patient's clinician that there are exceptional clinical circumstances which make the patient's case different from other patients with the same condition who are at the same stage of their disease, or when the request is for a treatment that is regarded as new or experimental and where there are no other similar patients who would benefit from this treatment. A detailed response, including the criteria considered in arriving at the decision, will be provided to the patient's clinician.

Invoice Validation. Invoice validation is an important process. It involves using your NHS number to check the ICB that is responsible for paying for your treatment. Section 251 of the NHS Act 2006 provides a statutory legal basis to process data for invoice validation purposes. We can also use your NHS number to check whether your care has been funded through specialist commissioning, which NHS England will pay for. The process makes sure that the organisations providing your care are paid correctly.

Supporting Medicines Management. ICBs support local GP practices with prescribing queries which generally don't require identifiable information. ICB pharmacists work with your practice to provide advice on medicines and prescribing queries, and review prescribing of medicines to ensure that it is safe and cost-effective. Where specialist support is required e.g. to order a drug that comes in solid form, in gas or liquid, the ICB medicines management team will order this on behalf of the practice to support your care.

Safeguarding. To ensure that adult and children's safeguarding matters are managed appropriately, access to identifiable information will be shared in some limited circumstances where it's legally required for the safety of the individuals concerned.

Our legal basis for processing For the General Data Protection Regulation (GDPR) purposes is: -
Article 6(1)(e) '…exercise of official authority…'.

For the processing of special categories data, the basis is: -
Article 9(2)(b) – 'processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law…'

Summary Care Record (SCR). The NHS in England uses a national electronic record called the Summary Care Record (SCR) to support patient care. It contains key information from your GP record. Your SCR provides authorised healthcare staff with faster, secure access to essential information about you in an emergency or when you need unplanned care, where such information would otherwise be unavailable.

Summary Care Records are there to improve the safety and quality of your care. SCR core information comprises your allergies, adverse reactions and medications. An SCR with additional information can also include reason for medication, vaccinations, significant diagnoses / problems, significant procedures, anticipatory care information and end of life care information. Additional information can only be added to your SCR with your agreement. For more information, see Additional Information in the SCR.

Please be aware that if you choose to opt-out of SCR, NHS healthcare staff caring for you outside of this surgery may not be aware of your current medications, allergies you suffer from and any bad reactions to medicines you have had, in order to treat you safely in an emergency.

You can exercise these rights by doing the following:

1. **Choose to have a Summary Care Record with all information shared**. This means that any authorised, registered and regulated health and care professionals will be able to see a detailed Summary Care Record, including Core and Additional Information, if they need to provide you with direct care.
2. **Choose to have a Summary Care Record with Core information only**. This means that any authorised, registered and regulated health and care professionals will be able to see limited information about allergies and medications in your Summary Care Record if they need to provide you with direct care.
3. **Choose to opt-out of having a Summary Care Record altogether**. This means that you do not want any information shared with other authorised, registered and regulated health and care professionals involved in your direct care. You will not be able to change this preference at the time if you require direct care away from your GP practice. This means that no authorised, registered and regulated health and care professionals will be able to see information held in your GP records if they need to provide you with direct care, including in an emergency.

Regardless of your past decisions about your Summary Care Record preferences, you will still have the same options that you currently have in place to opt out of having a Summary Care Record, including the opportunity to opt-back in to having a Summary Care Record or opt back in to allow sharing of Additional Information.

Local sharing via My Care Record. Your patient record is held securely and confidentially on our electronic system. If you require attention from a health professional such as an Emergency Department, Minor Injury Unit or Out Of Hours location, those treating you are better able to give appropriate care if some of the information from your GP patient record is available to them. This information can be locally shared electronically via My Care Record.

In all cases, the information is only used by authorised health and social care professionals in Cambridgeshire & Peterborough ICB area directly involved in your care. Your permission will be asked before the information is accessed, unless the health and social care user is unable to ask you and there is a clinical reason for access, which will then be logged.

Data Retention. We will approach the management of patient records in line with the Records Management NHS Code of Practice for Health and Social Care which sets the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England, based on current legal requirements and professional best practice.

Who are our partner organisations? We may also have to share your information, subject to strict agreements on how it will be used, with the following organisations:

- NHS Trusts
- Specialist Trusts
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Medical Examiner Service
- Voluntary Sector Providers
- Ambulance Trusts
- Integrates Neighbourhood Teams
- Integrated Care Board/Systems
- Hunts PCN
- Social Care Services
- Local Authorities
- Education Services
- Fire and Rescue Services

- Police
- Other ‘data processors’.

We will never share your information outside of health partner organisations without your explicit consent unless there are exceptional circumstances such as when the health or safety of others is at risk, where the law requires it or to carry out a statutory function. This means you will need to express an explicit wish not to have your information shared with the other NHS organisations; otherwise they will be automatically shared. We are required by law to report certain information to the appropriate authorities. This is only provided after formal permission has been given by a qualified health professional. There are occasions when we must pass on information, such as notification of new births, where we encounter infectious diseases which may endanger the safety of others, such as meningitis or measles (but not HIV/AIDS), and where a formal court order has been issued. Our guiding principle is that we are holding your records in strictest confidence.

Hunts Primary Care Network: The objective of primary care networks (PCNs) is for group practices together to create more collaborative workforces which ease the pressure of GP’s, leaving them better able to focus on patient care. Acorn Surgery is a member of the Hunts PCN. Other members of the network are: Hicks Group Practice, Priory Fields Surgery, Papworth Surgery.

Primary Care Networks form a key building block of the NHS long-term plan. Bringing general practices together to work at scale has been a policy priority for some years for a range of reasons, including improving the ability of practices to recruit and retain staff; to manage financial and estates pressures; to provide a wider range of services to patients and to more easily integrate with the wider health and care system.

This means the practice may share your information with other practices within the PCN to provide you with your care and treatment.

Service Evaluation: The PCN may carry out service evaluations in order to improve the quality and accessibility of primary care services. This may be carried out in a number of ways including telephone surveys, online surveys and interviews.

The legal basis for contacting you to take part -

Article 6, e) 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;”

Article 9, (h) processing is necessary for the purposes of preventive 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

To process the survey information, we collect from you we will only do so with your consent.
Article 6(1)(a) - Consent of the data subject (you)
Article 9(2)(a) – Explicit consent of the data subject. (you)’

Third Party Processors

To deliver the best possible service, the practice 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 as processors. 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 include:

- 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; document management services etc.
- Delivery services (for example if we were to arrange for delivery of any medicines to you).
- Medical Notes Storage
- Payment providers (if for example you were paying for a prescription or a service such as travel vaccinations).

Further details regarding specific third-party processors can be supplied on request to the Data Protection Officer as below

Accurx: As part of the Digital First National programme of work, GP Practices are required to provide a tool for patients to access primary care services.

The aim of the Accurx platform is to improve communications between healthcare staff and patients resulting in improved outcomes and productivity. The platform facilitates digital communications between the practice and our patients.

Using the Accurx platform will require the processing of special category data by Accurx, their sub-processors and by default the GP Practice as a Controller. This will include; exchanging and storing messages in relation to patients and medical staff, performing video consultations (these will not be recorded or stored) between healthcare staff and their patients This will allow you to respond to the Practice in multiple ways such as; free text, questionnaires and submitting images/documents.

If you have a non-urgent healthcare concern or need to contact the Practice for any medical or admin reason, click on the online via our website or via NHS app or via NHS website. Fill out the online form, which will then be reviewed and processed by our healthcare professionals to decide the right care for you. We will respond to every online request 2 workings days.

Accurx is approved by NHS England to be used by GP practices and the other systems involved in patient care. NHS England has a lengthy assurance process to make sure they meet the highest standards of safety and security. Your data is safe and is shared only with your GP Practice for the purposes of your direct care. Your data is stored and sent securely using industry best practices, and Accurx only collect the data that is necessary to allow your GP Practice to provide you with care.

The Practice uses the following Accurx features:
- Sending text messages
- Questionnaires
- Friends and Family test,
- online consultations,
- video consultations,
- AccuMail and Record Views

Accurx's privacy notice can be found on their website here: Accurx - Privacy Policy

Medical Examiner Service: Following the death of any patient, the Practice is required to inform the East of England NHS Trust's Medical Examiner Service.

Medical Examiner offices, based in acute NHS Trusts, provide independent scrutiny of all non-coronial deaths that occur within hospitals. Their role is now expanding to include deaths that take place in the community as well.

These offices are led by Medical Examiner, senior doctors from various specialties, including general practice who independently review deaths that are not immediately referred to the Coroner. Their focus is on supporting the bereaved, offering families and next of kin the opportunity to ask questions and express concerns about the care provided.

Medical Examiners conduct proportionate reviews of medical records and work closely with the doctors responsible for completing the Medical Certificate of Cause of Death (MCCD)

SystmOne Clinical System
TPP SystmOne is a clinical computer system used by our GP surgery to securely store and manage your personal health information. Developed by The Phoenix Partnership (TPP), SystmOne enables healthcare professionals to record, access, and share relevant medical data to provide safe and effective care. Your personal data, including contact details, medical history, medications, test results, and referrals, is processed in accordance with UK data protection laws. The system allows for the secure sharing of information with other authorised healthcare providers involved in your care, such as hospitals or community services, but only when necessary and with appropriate safeguards in place. TPP acts as a data processor on behalf of the Practice, and all data is hosted securely within the UK.

Accessing Your Medical Records: In accordance with the UK General Data Protection Regulation, patients (data subjects) have the right to access their data and any supplementary information held by this organisation. This is commonly known as a subject access request (SAR).

Data subjects have a right to receive:
- Confirmation that their data is being processes
- Access to their personal data
- Access to any other supplementary information held about them

Accessing your GP-held records via the NHS app or NHS website; As of April 2016, organisations have been obliged to allow patient's access to their coded health record online. As of October 2023, this service now enables the patient to view their full prospective medical record. Prior to accessing this information, you will have to visit the Practice and undertake an identity check before being granted access to your records. Alternatively you can request access online and provide proof of Identify. The document provided will be held for 7 days or until a staff member confirms the identity and then deleted.

Your GP medical record contains consultation notes based on conversations between you, your GP and their team: medicines prescribed to you; all test results including hospital investigations; allergies; vaccines; and your medical conditions along with documents that may have been sent from local hospitals, clinics or other agencies, eg the police. There is likely to be sensitive and personal information within your medical record. We are supportive of providing you with access to your record, but we wish to do this safely and make you aware that this is happening so that you can opt out, if you so wish. You may wish to speak with us first to understand what it is that you will see, and the risks which may be involved in having such confidential data either on your smartphone with the NHS app installed or online if other people might have access to that information through your devices. If you are in a difficult or pressured relationship for example, you may prefer your records to remain accessible only to those treating you, with them not appearing on your smartphone or online. Government has been clear that if a patient does not wish to have access, then we do not have to provide it. This is one reason why we have asked if you wish to opt out, or have it switched off for the time being. More information can be found on line via https://acornsurgery.com/policies/privacy-notice-gdpr-information/

In addition, you can make a request to be provided with copies of your health record. To do so, you must submit a SAR form. This can be submitted electronically and the SAR form is available on the organisation website. Alternatively, a paper copy of the SAR is available from reception. You will need to submit the form online or return the completed paper copy of the SAR to the organisation. Patients do not have to pay a fee for copies of their records.

- **Time frame;** Once the SAR form is submitted, this organisation will aim to process the request within 28 days; however, this may not always be possible.
- **Exemptions;** There may be occasions when the data controller will withhold information kept in the health record, particularly if the disclosure of such information is likely to cause undue stress or harm to you or any other person.
- **Data controller** At Acorn Surgery the data controller is Victoria Pilkington and should you have any questions relating to accessing your medical records, please ask to discuss this with the named data controller

Your right to withdraw consent for us to share your personal information (Opt-Out). If you are happy for your data to be extracted and used for the purposes described in this fair processing notice then you do not need to do anything. If you do not want your information to be used for any purpose beyond providing your care you can choose to opt-out. If you wish to do so, please let us know so we can code your record appropriately. We will respect your decision if you do not wish your information to be used for any purpose other than your care but in some circumstances we may still be legally required to disclose your data. There are two main types of opt-out.

National Data Opt-Out The National Data Opt-out is a service that allows patients to opt out of their confidential patient information being used for research and planning. The National Data Opt-out only applies to any disclosure of data for purposes beyond direct care, so having National Data Opt-out will not prevent your GP patient record being shared via GP Connect.

Type 1 Opt-Out
If you do not want information that identifies you to be shared outside the practice, for purposes beyond your direct care, you can register a 'Type 1 Opt-Out'. This prevents your personal confidential information from being used other than in particular circumstances required by law, such as a public health emergency like an outbreak of a pandemic disease.

Type 2 Opt-Out
NHS Digital collects information from a range of places where people receive care, such as hospitals and community services. If you do not want your personal confidential information to be shared outside of NHS Digital, for purposes other than for your direct care, you can register a 'Type 2 Opt-Out'. For further information about Type 2 Opt-Outs, please contact NHS Digital contact centre at enquiries@hscic.gov.uk referencing 'Type 2 Opt-Outs – Data Requests' in the subject line; or call NHS Digital on ***(0300) 303 5678****; or visit the website http://content.digital.nhs.uk/article/7092/Information-on-type-2-opt-outs .*

If you wish to discuss or change your opt-out preferences at any time please contact the Practice Manager.

Access to your information. Under the new General Data Protection Regulation (GDPR) 2018 everybody has the right to see, or have a copy, of data we hold that can identify you, with some exceptions. You do not need to give a reason to see your data. If you want to access your data you must make the request in writing. Under special circumstances, some information may be withheld. If you wish to have a copy of the information we hold about you, please contact the Practice.

Mobile Numbers & Email Addresses. If you provide us with your mobile phone number, we may use your email or mobile number this to notify you of appointments, send you booking links to make appointemnt, provide medical information notify you of patient education events and send health questionnaires to support your consultations. In addition clinicians and other members of the Practice team may communicate using your mobile number to request information via AccuRx clinical tool, or other health screening information. As this is operated on an 'opt out' basis we will assume that you give us permission to contact you via SMS if you have provided us with your mobile telephone number. Digital recordings of telephone calls will be held for no longer than three months from the date of the call unless for training and improvement purposes.

Change of Details. It is important that you tell the person treating you if any of your details such as your name or address have changed or if any of your details are incorrect in order for this to be amended. Please inform us of any changes so our records for you are accurate and up to date.

Correction of Errors. In-line with national legislation, individuals have the right to have access to their personal data which we process and store. Patient and Employees have the right to the rectification of said records in the instance that their records are inaccurate or incomplete.

- Where at all possible, in the instance that the Practice has appropriately shared that individual's records with any third-party we will inform this third-party of the rectification if appropriate.
- The Practice will respond to a request for rectification within one month. Should the request be complex this may be extended to two months, however, the individual will be informed in writing of the extension and the reasons why it is required within one month.

- To request for their records to be rectified Patients or staff should contact the Practice Manager as Data Security and Protection Lead with the request for rectification either verbally or in writing. If the rectification is due to the record being incomplete, then the individual should also provide the supplementary information to update the record.
- While the Practice assess request to rectify records, the processing of the data in question will be restricted. This will be done in line with our Right to Restrict Processing Procedure as outlined in our Record Keeping Policy.
- In the instance where the rectification request is refused, the reason will be explained in full and in writing within one month of the original request having been received.
- All individuals who have their rectification request refused will be informed of their legal rights to complain to the ICO and to seek a judicial remedy;
- In order to process your request for rectification, you might be asked to provide identifying documents so that we can authenticate that it is appropriate for you to update your data.

Right to Object: You have the right to object to the processing of your personal data if you believe it is being used inappropriately. While this is not an absolute right and there may be legal or legitimate reasons we must continue to process your data, we will consider your request carefully and respond within one month. In certain circumstances, we may be allowed to extend this period and will inform you if this applies.

Right to Withdraw Consent: If we process your personal data based on your consent—such as for research purposes or to send you information you've expressed interest in—you may withdraw your consent at any time. This will not affect any processing carried out before you withdrew consent.

Right to Erasure: In certain situations, such as where your data has been processed unlawfully, you have the right to request that we erase your personal data. We will assess your request and respond within one month, although this period may be extended in complex cases. If we agree to erase your data, we may retain limited information—such as your name—to ensure you are not contacted again in the future. You may request that we do not retain even this minimal information.

Right to Data Portability: You have the right to request that your personal data be transferred to another data controller, such as a new GP practice. We will support this through secure electronic transfer (e.g., GP2GP) and by forwarding any paper records where necessary.

Our Website: The only website this Privacy Notice applies to is the Acorn Surgery's website. If you use a link to any other website from the Surgery's website then you will need to read their respective Privacy Notice. We take no responsibility (legal or otherwise) for the content of other websites. The Practice**'**s website dose not uses cookies.

CCTV Recording: CCTV is installed on the Oaktree Centre premises covering both the external area of the building and the internal area, excluding consulting rooms. Images are held by the landlord Cambridge Community Services not the Practice.

Telephone Recording: The telephone call recording system in operation will record incoming and outgoing telephone calls and recordings may be used to investigate compliance with the Practice's policies and procedures, to provide further training, to support the investigation of complaints, to ensure the Practice complies with regulatory procedures and to provide evidence for any regulatory investigation. Call recordings are stored for no longer than three months unless required for training and monitoring purposes or to support incident and complaint investigations.

The NHS App

We use the NHS Account Messaging Service provided by NHS England to send you messages relating to your health and care. You need to be an NHS App user to receive these messages. Further information about the service can be found at the Privacy Notice for the NHS App managed by NHS England.

Notification. Acorn Surgery is registered with the Information Commissioners Office (ICO) to describe the purposes for which they process personal and sensitive information. We are a registered Data Controller and our registration can be viewed online in the public register at: http://ico.org.uk/what_we_cover/register_of_data_controllers

Complaints. If you have concerns or are unhappy about any of our services, please contact the Practice Manager. For independent advice about data protection, privacy and data-sharing issues, you can contact: The Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF - Phone: **0303 123 1113** Website: www.ico.gov.uk .

Further Information. Further information about the way in which the NHS uses personal information and your rights in that respect can be found here: https://www.england.nhs.uk/contact-us/privacy/privacy-notice/your-information/

The NHS Care Record Guarantee. The NHS Care Record Guarantee for England sets out the rules that govern how patient information is used in the NHS, what control the patient can have over this, the rights individuals have to request copies of their data and how data is protected under the Data Protection Act 1998. http://systems.digital.nhs.uk/infogov/links/nhscrg.pdf

The NHS Constitution. The NHS Constitution establishes the principles and values of the NHS in England. It sets out the rights patients, the public and staff are entitled to. These rights cover how patients access health services, the quality of care you'll receive, the treatments and programmes available to you, confidentiality, information and your right to complain if things go wrong. https://www.gov.uk/government/publications/the-nhs-constitution-for-england

NHS Digital. NHS Digital collects health information from the records health and social care providers keep about the care and treatment they give, to promote health or support improvements in the delivery of care services in England.
http://content.digital.nhs.uk/article/4963/What-we-collect
Transparency notice: how we use your personal data - NHS Digital
https://digital.nhs.uk/data-and-information/keeping-data-safe-and-benefitting-the-public/how-we-look-after-your-health-and-care-information

Reviews of and Changes to our Fair Processing Notice. We will keep our Fair Processing Notice under regular review.

May 2018; reviewed Jan 2020; updated Feb 2022, Nov 2023, Nov 2024, Feb 2025, reviewed and updated May 2025, updated July 2025, Oct 2025