

ALMONDBURY SURGERY

Patient & Visitor Privacy Notice

Data Controller: Almondbury Surgery

Introduction

At Almondbury Surgery, we understand how important it is to keep your personal and healthcare information safe and secure. We take our legal responsibility to protect your privacy and maintain absolute confidentiality very seriously.

The practice acts as a Data Controller, which means we are legally responsible for choosing how your data is used and ensuring it is looked after in the best possible way. This privacy notice explains why we collect information about patients, visitors, and members of the public, how we use it, and your legal rights.

Why We Collect Information About You

All clinicians and health and social care professionals caring for you keep detailed records about your health, history, and any treatment or care you receive within the NHS. These records are vital to ensure that you receive the safest and highest quality care possible.

Your records may be kept on paper or electronically and can include:

- **Basic Details:** Your name, address, email address, date of birth, NHS number, and next of kin.
- **Contact History:** Records of your appointments, clinic visits, and interactions with us.
- **Clinical Notes & Reports:** Notes regarding your health, diagnoses, medications, allergies, health conditions, treatments, A&E visits, or hospital stays.
- **Test Results:** Results of x-rays, laboratory tests, and diagnostic scans.
- **Third-Party Information:** Relevant details from other healthcare professionals or relatives who know you well and participate in your care.
- **Practice Visitors:** Basic information such as names and vehicle registration numbers.

Please Help Us Keep Records Accurate: It is essential that your details are correct. Please check your personal details when you visit and inform us immediately

of any changes to your contact information to avoid missing vital clinical correspondence.

Legal Basis for Processing Your Information

Under the UK General Data Protection Regulation (UK GDPR), the practice must establish a legal framework to process your data. Information regarding your physical and mental health, race, ethnicity, or religious beliefs is classified as Special Category Data and is bound by strict usage laws.

We process your data under the following legal bases:

For Personal Data:

- **Public Task:** The processing is necessary for the practice to perform its official functions and deliver healthcare services, with a clear basis in UK law.
- **Legal Obligation:** Necessary to comply with statutory law (outside of contractual requirements).
- **Consent / Explicit Consent:** Used when you give clear, specific permission for a particular purpose (e.g., telephone/video consultations or optional research).
- **Vital Interests:** Necessary in critical life-or-death situations where your life is at risk.

For Special Category (Sensitive Healthcare) Data:

- **Health or Social Care:** Necessary for medical diagnosis, the provision of health or social care, or treatment management under UK law.
- **Public Health:** Necessary for protecting against serious cross-border threats to health or ensuring high standards of healthcare (such as monitoring infectious diseases).
- **Vital Interests:** Used to protect an individual's life when they are incapable of giving consent.

How Your Information is Used

Direct Care Purposes

In general, your medical records are utilized to guide, manage, and coordinate the active care you receive. This ensures that:

- Your doctors, nurses, and allied health professionals have accurate, up-to-date information to safely assess your health.
- Clinicians have the necessary information to refer you to a specialist or another part of the NHS or social care network.
- We can securely offer you a consultation via telephone or videoconferencing if appropriate (accepting the invitation acts as consent).

- **Communication:** By providing us with your contact details, you agree to the practice contacting you via letter, phone call, voicemail, email, or SMS text messages regarding your appointments and healthcare.

Indirect Care & Secondary Purposes

We also use de-identified, aggregated, or pseudonymised information to support the wider NHS, which includes:

- Reviewing and auditing the quality and safety of care we provide to ensure it hits the highest standards.
- Training and educating healthcare professionals.
- Planning, commissioning, and structuring local healthcare services to meet future patient demands.
- Investigating patient queries, feedback, or formal complaints.
- Conducting health research and development (only with your specific consent).

When Do We Share Information About You?

Everyone working within or for the NHS has a strict legal and contractual duty to keep your information entirely confidential. Anyone who receives information from us is bound by the same legal duty.

We share information with various partners to facilitate your care, including:

Direct Care Partners:

- NHS Trusts, hospitals, and ambulance services involved in your active treatment.
- Other General Practitioners (GPs) and our local Primary Care Network practices.
- NHS England, NHS Digital, and local Integrated Care Boards.
- Social Care Services, Local Authorities, or Education Services where there is a genuine need and joint care is provided for your benefit.
- Partnered voluntary or private sector providers working directly with the NHS (e.g., community pharmacies, dentists, opticians, and care homes).

Secondary / Indirect Care Sharing:

- **OpenSAFELY COVID-19 Service:** A secure, open-source platform managed by NHS England that uses pseudonymised data for ongoing health surveillance, monitoring risk factors, and predicting healthcare service demands.

- **Statutory Requirements:** We may share identifiable information without consent if forced to by law, such as reporting a legally notifiable disease to public health authorities.

Managing Your Choices

Refusing or Withdrawing Consent

In instances where information sharing relies purely on your explicit or implied consent, you hold the right to refuse or withdraw that consent at any time. Please note that choosing not to allow data sharing with other health and social care professionals may make providing treatment highly difficult or completely unavailable. If you object, we will explicitly record your choice within your records so all clinical staff are fully aware of your wishes.

National Data Opt-Out

The information collected about you across health and care services can be used by other organizations to help with research, planning services, monitoring safety, and developing new treatments.

If you do not want your confidential patient information to be shared for these planning and research purposes, you can choose to opt out. Registering an opt-out will not affect your individual, direct care in any way. Your information will never be sold to insurance companies or used for marketing purposes without your explicit agreement.

- To learn more or set your data preferences, visit www.nhs.uk/your-nhs-data-matters.

Additional Tools We Use

Call Recording

All telephone calls made to and from the practice are routinely recorded. We do this to ensure staff comply with correct procedures, maintain quality control, deliver training, improve services, and prevent crime or protect our staff.

CCTV

We employ surveillance cameras (CCTV) on and around the practice premises. This is designed to safeguard patients, staff, and visitors, protect practice property, deter unlawful activity, and assist staff in spotting individuals who require physical assistance.

Data Security, Retention, and Freedom of Information

We protect your data across all formats (computerised or paper) using strict physical and electronic security controls. The practice partners have appointed a Senior Information Risk Owner to oversee all information assets and risk management.

- **Retention:** We adhere to the NHS Records Management Code of Practice. Records are never kept longer than necessary and are destroyed under confidential, secure conditions once their retention period is met.
- **Freedom of Information:** The Freedom of Information Act 2000 gives the public the right to request certain non-personal information held by the practice. Freedom of Information requests do not apply to your personal medical records.

Your Individual Rights

Under the UK GDPR, you have the right to:

1. **Be Informed:** To know why, where, and how your information is handled.
2. **Access Your Data:** To request a copy of the information we hold about you (a Subject Access Request). This is free of charge in most cases and fulfilled within 1 month. This right extends to requesting a copy of recorded CCTV images of yourself.
3. **Rectification:** To have inaccurate or incomplete data corrected.
4. **Restriction / Objection:** To restrict or object to how your data is used or shared.
5. **Data Portability:** To receive your electronic data in a commonly used format.

Note: The right to erasure ("the right to be forgotten") does not apply to official NHS medical records or data processed for public health purposes.

Governance, Queries, and Complaints

Caldicott Guardian

Our Caldicott Guardian is responsible for protecting the confidentiality of patient information and enabling appropriate information sharing.

- **Caldicott Guardian:** Dr. Alison Brandao

Data Protection Officer

Our independent Data Protection Officer monitors our compliance with data laws.

- **DPO:** Helen Holt
- **Email:** Helen.Holt@this.nhs.uk
- **Address:** Unit 13, Ainley Bottom, Ainley Industrial Estate, Elland, HX5 9JP

Raising a Concern

If you have any concerns regarding how your records are managed at the practice, please speak directly with the Business Manager.

You also retain the right to lodge an independent complaint at any time with the UK data protection regulator:

- **Authority:** Information Commissioner's Office (ICO)
- **Address:** Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
- **Telephone:** 0303 123 1113
- **Website:** www.ico.org.uk