Victoria Medical Centre
12-28 Glen Street
Hebburn
Tyne & Wear
NE31 1NU
T: 0191 483 2106
W: www.victoriamedicalcentrehebburn.nhs.uk

Patient Privacy Notice

This Privacy Notice applies to patients and service users of Victoria Medical Centre. Separate privacy notices are available for employees, workers, volunteers, contractors and job applicants on request.

Introduction

Victoria Medical Centre is committed to protecting your privacy and ensuring your personal information is handled securely and confidentially.

This Privacy Notice explains how we collect, use, store and share your personal information when you receive healthcare services from the Practice.

The Practice is the Data Controller for the information we hold about you and processes personal information in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the common law duty of confidentiality and relevant NHS legislation.

Contact Details

Victoria Medical Centre
12-28 Glen Street
Hebburn
Tyne & Wear
NE31 1NU
T: 0191 483 2106
E: nencicb-styn.victoria-medical-centre@nhs.net
W: www.victoriamedicalcentrehebburn.nhs.uk

Data Protection Officer

North East and North Cumbria Integrated Care Board Data Protection Team
Email: liane.cotterill@nhs.net

Information Commissioner's Office (ICO)

Website: www.ico.org.uk
Telephone: 0303 123 1113

Information Governance Leads

The Practice has appointed:

- A Caldicott Guardian, responsible for protecting the confidentiality of patient information and enabling appropriate information sharing.

- A Senior Information Risk Owner (SIRO), responsible for information risk and data security governance within the Practice.

Further information is available on request.

ICO Registration Number

Victoria Medical Centre is registered with the Information Commissioner's Office (ICO) as a Data Controller.

Registration Number: Z7693158

Confidentiality Statement

Everyone working for the Practice is subject to a duty of confidentiality and receives regular information governance and data protection training.

Legal Disclosure

We may disclose information without consent where we are required to do so by law, court order, safeguarding obligations, public health legislation, prevention or detection of crime, or where there is a serious risk of harm to an individual or the public.

We may disclose information without consent where required or permitted by law, where there is an overriding public interest, or where there is a legal obligation to do so.

Children and Young People

We recognise that children and young people have the same duty of confidentiality owed to them as adult patients. Information will be shared with parents, guardians or others only where appropriate, with consent, where there is a lawful basis to do so, or where disclosure is considered necessary in the child's best interests.

Information We Collect

We collect and process information necessary to provide healthcare services and meet our legal obligations.

This may include:

- Name, address and contact details
- Date of birth
- NHS number
- Next of kin details
- Medical history
- Consultation notes
- Test results and investigations
- Prescriptions and medication records
- Appointment information
- Correspondence relating to your care
- Information provided by hospitals, community services and other healthcare providers
- Images, recordings or documents relevant to your healthcare

How We Obtain Information

Information is obtained directly from you, from healthcare professionals involved in your care, hospitals, community services, social care organisations, NHS systems and other organisations where there is a lawful basis to share information with the Practice.

Why We Use Your Information

We use your information to:

- Provide safe and effective healthcare
- Assess and manage your treatment
- Arrange referrals to other healthcare providers
- Communicate with you regarding appointments and care
- Manage complaints and compliments
- Safeguard children and vulnerable adults
- Meet legal and regulatory requirements
- Improve the quality and safety of services
- Undertake clinical audit and service planning
- Prevent and detect fraud or crime

Lawful Basis for Processing

We process personal information under:

- Article 6(1)(e) UK GDPR - Public task
- Article 9(2)(h) UK GDPR - Delivery of health or social care
- Article 9(2)(i) UK GDPR - Public health purposes
- Article 6(1)(c) UK GDPR - Legal obligation (where applicable)

How We Share Information

Your information may be shared with organisations involved in your direct care where there is a legitimate need to do so.

This may include:

- NHS hospitals
- Community healthcare services
- Mental health services
- Out-of-hours providers
- Ambulance services
- Community pharmacies
- Social care services
- Integrated Care Boards (ICBs)
- NHS England
- Primary Care Network (PCN)
- Other GP practices where appropriate

We only share the minimum necessary information required for the purpose.

Sharing Information With Family Members and Representatives

We will generally only discuss a patient's confidential information with the patient themselves, unless:

- The patient has given permission;
- The patient lacks capacity and disclosure is considered to be in their best interests;
- There is another legal basis permitting disclosure.

Our staff may ask questions to confirm the identity and authority of anyone requesting information on behalf of a patient.

Safeguarding

The Practice may share information without consent where there is a lawful basis to do so for safeguarding purposes, including concerns relating to:

- Children
- Vulnerable adults
- Serious harm
- Public safety

Information is shared only with appropriate agencies and professionals.

Summary Care Record

Most patients in England have a Summary Care Record (SCR).

The Summary Care Record contains key medical information and allows authorised healthcare professionals involved in your care to access important information when required.

You can choose to opt out of having a Summary Care Record.

GP Connect

The Practice participates in GP Connect.

GP Connect enables authorised healthcare professionals involved in your care to access relevant information from your GP record where appropriate and lawful to do so.

Shared Care Records

Patients who wish to understand more about local shared care record arrangements, including any options available to object, can contact the Practice or the Integrated Care Board.

Referrals

Where clinically appropriate, information may be shared through NHS referral systems, including the NHS e-Referral Service, to enable referrals to hospitals and other healthcare providers.

National Data Opt-Out

The NHS National Data Opt-Out allows patients to choose whether their confidential patient information is used for research and planning purposes.

The National Data Opt-Out does not apply where information is used for your individual care and treatment.

For further information visit:
www.nhs.uk/your-nhs-data-matters

Digital and Communication Systems

To support the delivery of healthcare services, the Practice uses a range of NHS-approved systems and service providers.

These may process personal information on behalf of the Practice under contractual agreements and only where necessary for healthcare delivery, communication, administration, legal obligations, security or service improvement.

Examples include:

- EMIS Web clinical system
- EMIS Patient Check-In services
- Accurx communication platform
- Surgery Connect/X-on telephony platform
- NHS App services
- Jayex patient call and waiting room information systems
- INRstar anticoagulation management system
- Microsoft 365
- NHS Mail

The Practice may also use other approved NHS and healthcare technology suppliers where necessary to support patient care and business operations.

Data Processors

The Practice uses carefully selected third-party suppliers and NHS-approved service providers to support healthcare delivery, administration, communication, information technology, security and business operations.

These organisations act either as Data Processors on behalf of the Practice or as independent Data Controllers where appropriate.

We ensure appropriate contracts, data sharing agreements and security measures are in place before information is shared.

The Practice uses carefully selected third-party providers.

Online Forms

Information submitted through online consultation tools, website forms or digital services is processed securely and incorporated into the patient's medical record where relevant to their care.

Online Access to Records

Patients may access parts of their medical record using approved online services including the NHS App. Access is provided in accordance with NHS guidance and may be restricted where necessary for safeguarding, confidentiality or legal reasons.

International Transfers

Where information is processed using cloud-based providers, appropriate safeguards and contractual protections are implemented to ensure compliance with UK GDPR and applicable data protection legislation.

Text Messages, Emails and Letters

The Practice may contact you by:

- Telephone
- SMS text message
- Email
- NHS App notifications
- Letter

Please ensure your contact details remain up to date. Communications may contain personal information relating to your healthcare and are sent on the basis that they are necessary for the provision of healthcare services, administrative purposes, or where you have indicated a preference for a particular communication method.

Patient Communication Preferences

Patients may inform the Practice of their preferred communication methods. While we will endeavour to accommodate preferences where possible, certain communications may still need to be provided where required for patient safety, legal or operational reasons.

Information Security

The Practice uses technical and organisational security measures to protect personal information from unauthorised access, loss, misuse, alteration or disclosure. Access to information is restricted to authorised individuals who require it for legitimate purposes.

The Practice complies with the NHS Data Security and Protection Toolkit requirements.

Data Breach

Any actual or suspected data breaches are investigated in accordance with the Practice Data Security and Protection procedures and, where required, reported to the Information Commissioner's Office and other appropriate bodies.

Telephone Call Recording

Telephone calls to and from the Practice may be recorded for:

- Staff training
- Quality assurance
- Patient safety
- Complaint investigation
- Service improvement
- Prevention and detection of crime

Access to recordings is strictly controlled and restricted to authorised personnel.

CCTV

CCTV is in operation at Victoria Medical Centre for the purposes of:

- Safety and security of staff, patients and visitors
- Prevention and detection of crime
- Investigation of incidents
- Protection of property and assets

CCTV is not installed within consulting rooms, treatment rooms or toilets.

Recordings are accessed only by authorised individuals in accordance with the Practice CCTV Policy.

CCTV recordings are normally retained for 30 days before automatic deletion unless required for the investigation of an incident, complaint or legal matter.

Waiting Room Information Screens

The Practice uses waiting room display and patient call systems to assist with patient flow and communication.

These systems are configured to minimise the use of personal information and are used solely for operational and service delivery purposes.

Research, Audit and Planning

The Practice may contribute information for approved audit, planning, commissioning and research purposes where there is a lawful basis for doing so.

Appropriate safeguards are always applied.

How Long We Keep Information

The Practice retains records in accordance with the NHS Records Management Code of Practice and other applicable legal requirements including the current NHS Records Management Code of Practice for Health and Social Care.

Records are securely destroyed when retention periods expire.

Your Information Rights

You have the right to:

- Request access to your information
- Request correction of inaccurate information
- Request restriction of processing in certain circumstances
- Object to processing where applicable
- Request information about how your data is used
- Lodge a complaint about how your information is handled

Some rights may be limited where the Practice has a legal obligation to retain or process information.

Subject Access Requests (SAR)

You are entitled to request access to information held about you.

SAR can be submitted to the Practice Manager using the Practice contact details provided within this Privacy Notice. Requests may be made verbally or in writing.

Most requests are completed free of charge and within one calendar month.

Identification may be requested before information is released.

Certain information may be withheld where disclosure would:

- Cause serious harm to the physical or mental health of any person;
- Reveal information relating to another individual who has not consented;
- Prejudice the prevention or detection of crime;
- Be exempt under applicable legislation.

Website and Cookies

Our website may use cookies and similar technologies to ensure functionality, improve user experience and collect anonymised usage information. Further information is available within the Practice Website Cookie Policy.

Accuracy of Information

Patients are responsible for informing the Practice of any changes to their contact details or personal circumstances. The Practice relies on the accuracy of information provided by patients and third parties involved in their care.

Concerns and Complaints

If you have concerns about how your personal information has been used, please contact the Practice in the first instance.

If you remain dissatisfied, you may contact:
Information Commissioner's Office (ICO)
Wycliffe House
Water Lane
Wilmslow
SK9 5AF
Website: www.ico.org.uk
Telephone: 0303 123 1113

Changes to This Privacy Notice

This Privacy Notice will be reviewed periodically and updated where necessary to reflect changes in legislation, guidance or Practice processes.

Last Reviewed: October 2026
Next Review Date: October 2027