Nimbuscare Privacy Notice

Version	Date	Author	Description of Change
1	31/03/26	Jennifer Butcher Associate Director of Governance and Quality Compliance	Full rewrite- prior version retired
Approved Date:		March 2026	
Approved By:		Associate Director of Governance and Quality Compliance, DPO, Medical Director	
Review Date:		March 2027	
Synopsis:		This privacy notice explains how Nimbuscare uses personal and health information to deliver safe, effective, and coordinated care across its services. It outlines what information is collected, how it is used and shared with partner organisations, and the legal basis for this processing, including support for neighbourhood working, case finding, and research. It also explains how information is protected and your rights in relation to your data.	
The implementation of this document aligns with the Equality Act 2010, with consideration of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation and human rights to ensure fair application. Nimbuscare operate within a Just Culture Framework, and our policies, procedures and SOPs are developed in line with the Patient Safety Incident Response Framework (PSIRF), ensuring we are Safe, Caring, Effective, Responsive and Well-Led.			

CONTENTS

INTRODUCTION: WHO WE ARE AND WHAT WE DO

Nimbuscare is a not-for-profit organisation providing both NHS and private healthcare services, delivering high-quality care to local populations.

We work collaboratively with system partners to design and deliver innovative and sustainable healthcare services. As a provider within the health and care system, our aim is to improve population health outcomes and patient experience through integrated, person-centred care.

Nimbuscare Limited is a federation of 11 GP practices across York:

1. Dalton Terrace
2. Elvington Medical Practice
3. Front Street Surgery
4. Haxby Group
5. Jorvik Gillygate
6. MyHealth
7. Old School Medical Practice
8. Pocklington Group Practice
9. Priory Medical Group
10. Unity Health
11. York Medical Group

We work in partnership with a range of NHS organisations and other healthcare providers, including hospitals and your registered GP practice, to deliver both NHS and non-NHS services across North Yorkshire.

In line with UK data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and in accordance with NHS information governance standards, we use and share relevant information from your health record to support your care.

To ensure you receive safe, effective, and coordinated care, we may access and update your shared patient record. This allows authorised healthcare professionals involved in your care to view relevant information, supporting continuity of care and informed clinical decision-making.

We monitor the performance of services that we sub-contract or deliver to make sure that they are safe, provide high-quality care, meet the needs of local people and provide value for money. Part of this performance monitoring role includes responding to any concerns from our patients about these services.

WHAT IS A PRIVACY NOTICE AND WHY DO WE PROVIDE IT?

A privacy notice explains what information Nimbuscare collects about you and how your personal data is used.

Under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, organisations must process personal data lawfully, fairly, and transparently. This applies to all uses of your personal information.

Nimbuscare is required by law to provide you with this information so that you understand how your data is collected, used, stored, and shared.

This means we must:

- Have a lawful basis for collecting and using your personal data
- Only use your information for specific, legitimate purposes
- Ensure your information is handled in a way that is appropriate and does not cause harm
- Be open and transparent about how your data is used
- Handle and protect your data in line with relevant legislation, guidance, and security standards
- Only use personal data where it is necessary and lawful to do so

This privacy notice also explains:

- Why we collect your personal and health information
- How your information is used
- The lawful basis for processing your information
- Who your information may be shared with and why
- How long your information is kept
- Your rights in relation to your personal data

If you have any questions about this privacy notice or how your information is used, you can contact Nimbuscare for further information.

YOUR PRIVACY MATTERS

Nimbuscare is committed to protecting your privacy and handling your information lawfully, fairly, securely, and transparently.

We use your information to:

- Provide care and treatment
- Coordinate care across services and organisations
- Maintain safe and effective services
- Meet legal, regulatory, professional, and contractual obligations
- Support service planning, quality assurance, audit, and improvement
- Support approved research and innovation, where appropriate

We will only use the minimum necessary information for each purpose and will only share information where there is a lawful basis to do so.

INFORMATION WE COLLECT AND HOLD

We may collect and hold information about you such as:

- Your name, address, date of birth, NHS number, and contact details
- Information about your health, treatment, diagnoses, medications, allergies, and care plans
- Details of appointments, referrals, assessments, test results, and communications
- Information about the services you receive from Nimbuscare or partner organisations
- Relevant social or care information needed to support safe care or to meet contractual obligations.
- Safeguarding information where relevant
- Administrative and operational information, such as eligibility, service use, and funding-related details where applicable
- Records of telephone calls, messages, feedback, complaints, events , or concerns where relevant to care, service management, or safety

Your information may be held in electronic records, paper records, call recordings, secure digital systems, and other approved record systems used to deliver and manage services.

TYPES OF INFORMATION WE USE

Nimbuscare uses and processes different types of information, including:

- Identifiable data: information that directly identifies you, such as your name, address, contact details, NHS number, postcode, and date of birth

- Pseudonymised data: information where identifying details have been replaced with a code so individuals cannot be directly identified without additional information

- Anonymised data: information that does not identify you and cannot reasonably be used to identify you

- Aggregated data: grouped information that shows trends or patterns without identifying individuals

Where possible, we use anonymised, aggregated, or pseudonymised data rather than identifiable information.

HOW WE USE YOUR INFORAMATION

We may use your information to:

- Assess your needs and provide care and treatment
- Make clinical decisions and maintain accurate clinical records
- Refer you to the most appropriate service or professional
- Coordinate your care with your GP practice and other organisations involved in your care
- Manage follow-up, reviews, recalls, and ongoing support
- Communicate with you about appointments, care, and services
- Safeguard children and adults at risk
- Investigate incidents, complaints, concerns, and claims
- Undertake clinical audit, service evaluation, and quality improvement
- Train staff and assure service quality, where lawful and proportionate
- Plan, develop, and improve services
- Meet legal and regulatory obligations
- Support research, innovation, and evaluation where lawful and appropriate

OUR LAWFUL BASIS FOR USING YOUR INFORMATION

Nimbuscare processes personal information lawfully, fairly, and transparently in line with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Human Rights Act 1998, the Health and Social Care Act 2012, the common law duty of confidentiality, and relevant NHS guidance and codes of practice. Health and care organisations commonly rely on the lawful bases and conditions relating to public functions, legal obligations, and the provision and management of health or social care. We are committed to being open about how your information is used and to ensuring that personal confidential data is handled securely, appropriately, and in ways you would reasonably expect in the delivery of healthcare. Health records may be held electronically, on paper, or in a combination of both.

Depending on the purpose, Nimbuscare may rely on one or more of the following:

For personal data under Article 6 UK GDPR:

- Article 6(1)(c) – processing is necessary for compliance with a legal obligation
- Article 6(1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority

For health and other special category data under Article 9 UK GDPR:

- Article 9(2)(h)-processing is necessary for the provision or management of health or social care or treatment
- Article 9(2)(i) -processing is necessary for reasons of public interest in the area of public health
- Article 9(2)(j)-processing is necessary for archiving, research, or statistical purposes, where appropriate safeguards are in place

In some situations, Nimbuscare may also rely on:

- Consent: where this is the appropriate legal basis

- Vital interests: for example in an emergency
- Legal claims: where information is needed for the establishment, exercise, or defence of legal claims

Where the common law duty of confidentiality applies, we will also ensure that confidential patient information is used or shared lawfully and appropriately.

WHO IS THE DATA CONTROLLER?

Nimbuscare Limited is a registered data controller and is responsible for deciding how personal information is used in relation to many of the services we provide. Our registration reference is ZA439119 and our registration can be viewed online in the public register at www.ico.gov.uk.

However, because Nimbuscare works across a range of service models, our role is not always the same.

Depending on the service, Nimbuscare may act as:

- An independent Data Controller, where we provide direct care and determine how information is used
- A Joint Controller with one or more partner organisations, where we jointly determine how information is used in an integrated service
- A Data Processor, in limited circumstances where we process information only on behalf of another organisation acting on its instructions

In most situations where Nimbuscare delivers direct care, records assessments, makes clinical decisions, or shares relevant information for care coordination, Nimbuscare will act as a Data Controller.

HOW WE WORK WITH GP PRACTICES AND PARTNER ORGANISATIONS

Nimbuscare is a federation of member GP practices and also works with a wide range of NHS and partner organisations.

This means we may use and share information with organisations involved in your care or in supporting safe and effective services, including:

- Your registered GP practice
- NHS Trusts and Foundation Trusts
- Community health providers
- Pharmacies
- Primary Care Networks
- Integrated Care Boards
- Integrated Care Systems
- NHS England and other national NHS bodies
- Local authorities
- Social care services
- Ambulance services

- Voluntary and community sector organisations involved in your care
- Independent providers involved in care delivery
- Safeguarding partners, including police, education, and relevant local authority services where required

We only share relevant information, with appropriate safeguards, and only where there is a lawful basis.

SHARED CARE RECORDS AND DIRECT CARE

Nimbuscare clinicians and authorised staff may access and update relevant parts of your shared health record where this is necessary to provide you with safe, effective, and coordinated care.

This may include information held within systems such as SystmOne or other approved NHS systems used to support direct care. Where shared care records are in use, relevant professionals involved in your care may be able to view information needed to understand your health needs, treatment, medications, allergies, and care history.

Shared care supports continuity, reduces duplication, improves safety, and helps clinicians make informed decisions. We only access information on a need-to-know basis and in line with professional, legal, and organisational requirements.

NEIGHBOURHOOD WORKING, MDT'S INTEGRATED TEAMS AND CASE FINDING

Nimbuscare works within neighbourhood and integrated models of care with member GP practices and other partners. This may include multidisciplinary teams, integrated neighbourhood teams, frailty services, urgent community response, care home support, mental health support, coordination hubs, virtual wards, and other collaborative services.

As part of this work, information may be used to:

- Identify people who may benefit from early intervention, proactive support, or review
- Coordinate care across teams and organisations
- Support multidisciplinary team discussions and decision-making
- Manage caseloads within specific services such as frailty or community-based support
- Target support to patients with the greatest clinical need or risk

For some services, such as frailty pathways, Nimbuscare may hold and manage a defined caseload for the duration of that service, even where the patient remains registered with one of our member GP practices.

For other services, Nimbuscare may not hold an ongoing caseload but may still access and use relevant information in order to assess, triage, coordinate, or deliver a specific episode of care.

Where case finding or proactive review is undertaken across member practices, this will be done to support care delivery, service coordination, prevention, quality improvement, or lawful planning activity, using the minimum necessary information and appropriate governance controls.

SUBCONTRACTED, PRIME PROVIDER, AND COMMISSIONED SERVICES

Nimbuscare delivers some services directly, subcontracts some services to other organisations, and in some cases provides services as a subcontractor to another organisation.

This means information may be shared within agreed contractual, legal, and information governance arrangements to enable services to be delivered safely, effectively, and lawfully.

Where Nimbuscare acts as a lead or prime provider, we may monitor quality, safety, performance, outcomes, and patient experience across the services delivered on our behalf.

Where another organisation commissions or leads a service that Nimbuscare delivers, we may use or share information in line with the agreed service model and each organisation's legal responsibilities.

NON-CLINICAL AND SUPPORT SERVICES

Nimbuscare also uses information to support non-clinical functions necessary for safe and effective service delivery. This may include:

- Appointment booking and scheduling
- Communications and reminders
- Interpretation and accessibility support
- Patient transport and logistics
- Lone working and staff safety systems
- Digital consultation or triage systems
- Telephone systems and call recording
- Feedback and service experience tools
- Website and online contact functions
- Workforce, governance, and operational systems where relevant to service delivery

We will only use and share the information necessary for the specific function.

RESEARCH, INNOVATION AND EVALUATION

Nimbuscare may use your contact details to invite you to take part in research, where this is appropriate and lawful.

Nimbuscare may support or participate in research, innovation, service evaluation, and pilot activity to improve care, understand outcomes, and contribute to the development of health services.

This may include the use of:

- Anonymised data
- Pseudonymised data
- Identifiable information, where lawful and appropriate

Where identifiable information is used for research, this will only happen where there is an appropriate legal basis, suitable approvals, and appropriate safeguards. Depending on the nature of the project, this may include patient consent, ethics approval, Confidentiality Advisory Group support where applicable, or another lawful route.

Where possible, research and evaluation will use anonymised or pseudonymised information rather than directly identifiable data.

If Nimbuscare invites you to take part in research, you will usually be given separate information about that specific project.

CLINICAL AUDIT, QUALITY IMPROVEMENT, AND SERVICE EVALUATION

Nimbuscare may review records and service information to assure quality, improve safety, monitor outcomes, learn from incidents, and evaluate the effectiveness of services.

This may include:

- Clinical audit
- Case review
- Peer review
- Complaints review
- Incident investigation
- Service evaluation
- Patient safety learning
- Performance monitoring

This work supports the management of healthcare services and is an important part of ensuring safe, effective, and high-quality care.

Article 9.2.h is applicable to the management of healthcare services and "permits processing necessary for the purposes of medical diagnosis, provision of healthcare and treatment, provision of social care and the management of healthcare systems or services or social care systems or services.'" No consent is required to audit clinical notes for this purpose.

Furthermore, compliance with Article 9(2)(h) requires that certain safeguards are met. The processing must be undertaken by or under the responsibility of a professional subject to the obligation of professional secrecy or by another person who is subject to an obligation of secrecy.

Auditing clinical management is no different to a multi-disciplinary team meeting discussion whereby management is reviewed and agreed. It would be realistically impossible to require consent for every patient reviewed that is unnecessary. It is also prudent to audit under Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17: Good Governance.

SAFEGUARDING

Nimbuscare is committed to safeguarding children, young people, and adults at risk.

Where there are concerns about abuse, neglect, or harm, we may share relevant information with appropriate safeguarding partners, such as local authorities, police, healthcare providers, and other agencies, where this is necessary and lawful.

We will only share the minimum information required and will do so in line with our legal duties, professional responsibilities, and safeguarding obligations

WHEN WE MAY SHARE INFORMATION WITHOUT YOUR CONSENT

There are circumstances where Nimbuscare may need to use or share your information without asking for your consent first. These may include:

- Where there is a risk of serious harm to you or another person
- Safeguarding concerns or investigations
- Where there is a legal requirement to share information
- Where a court order or other lawful instruction applies
- Where communicable disease reporting or other public health requirements apply
- Where serious crime prevention or detection requires disclosure
- Where information is needed for the management of health or care services and the law permits this

Where possible, we will still be open about how information is used.

Some examples are:

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

THIRD PARTY PROCESSORS

Nimbuscare uses a range of approved third party suppliers and digital systems to support the delivery of our services. These may include providers of:

- Clinical systems
- Referral systems
- Call handling and telephony
- Appointment and communication platforms
- Digital consultation and triage tools
- Records hosting or infrastructure
- Incident, lone working, or safety systems
- Survey and feedback tools
- Accessibility or interpretation systems
- Website hosting and analytics

- Approved devices and remote monitoring systems

Where a third-party processes personal data on our behalf, we will have an appropriate contract or data processing agreement in place and require them to keep the information secure and only use it in accordance with our instructions.

Because our digital systems and suppliers may change over time, Nimbuscare should maintain a separate processor and systems schedule alongside this privacy notice.

NATIONAL OPT-OUT FACILITY

The National Data Opt-Out allows you to choose whether your confidential patient information is used for purposes beyond your individual care, such as research and planning. It does not apply to information used for your direct care and treatment.

Nimbuscare will apply the National Data Opt-Out where it is applicable.

Further information, including how to set or change your preference, is available via the NHS website. Useful resources include:

Understanding the national data opt-out.

Setting or changing a national data opt-out choice.

Make a choice about sharing data from your health records.

HOW LONG WE KEEP YOUR INFORMATION

Nimbuscare keeps records in line with the NHS Records Management Code of Practice 2023 and any other legal, regulatory, contractual, and professional requirements that apply. This Code provides the framework for how long records should be kept across health and care organisations in England.

We do not keep personal information for longer than necessary.

Further information can be found on record management here: NHSE – Records Management Code of Practice 2023

ANONYMISED INFORMATION

Sometimes we may provide information about you in an anonymised form. Such information is used analyse population- level heath issues and helps the NHS to plan better services. If we share information for these purposes, then none of the information will identify you as an individual and cannot be traced back to you.

HOW WE KEEP YOUR INFORMATION SAFE

Nimbuscare takes the security of your information seriously.
We use technical and organisational measures to protect information, including:

- Role-based access controls
- Confidentiality and information governance training
- Secure nhs and approved digital systems
- Passwords, encryption, and authentication controls where appropriate
- Audit trails and monitoring
- Information sharing agreements and contracts
- Policies for records management, access, retention, and incident handling

Only authorised staff, contractors, and approved partners with a legitimate need to know will access your information.

Nimbuscare has a duty to protect your confidentiality. All staff, contractors, and partners are required to handle your information in line with data protection law, the common law duty of confidentiality, and NHS standards.

Staff receive regular training and are only given access to information necessary for their role.
We follow the Caldicott Principles, which support both protecting confidentiality and sharing information appropriately where it is in your best interests.

INTERNATIONAL TRANSFERS AND STORAGE

Nimbuscare aims to ensure that personal data is processed within the UK. If any supplier stores or accesses information outside the UK, this will only happen where lawful and appropriate safeguards are in place.

YOUR RIGHTS

Under data protection law, you have a number of rights in relation to your personal information. These include:

- The right to be informed about how your information is used
- The right to request access to the information we hold about you
- The right to request correction of inaccurate or incomplete information
- The right to object to the use of your information in certain circumstances
- The right to request restriction of how your information is used in certain circumstances
- The right to data portability, where applicable
- Rights relating to automated decision-making and profiling, where relevant

These rights are not absolute and may be limited where the law allows, particularly where information is required for the provision of healthcare, safeguarding, or to meet legal obligations.

RIGHT TO OBJECT

You have the right to object to the use of your personal information in certain circumstances. Where you object, we will carefully consider your request and respond within one month (this may be extended where permitted by law).

Please note that this is not an absolute right. In some cases, we may continue to use your information where there are legitimate or legal grounds to do so, such as for the provision of care, safeguarding, or legal requirements.

RIGHT TO WITHDRAW CONSENT

Where Nimbuscare relies on your consent to use your personal information (for example, for certain types of research or optional communications), you have the right to withdraw that consent at any time.

Withdrawing consent will not affect the lawfulness of any processing carried out before your consent was withdrawn.

RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN)

In certain circumstances, you have the right to request that we erase your personal information. This may apply where:

- Your information has been processed unlawfully
- The information is no longer necessary for the purpose it was collected
- You have withdrawn consent and there is no other legal basis for processing

Requests for erasure should be made to Nimbuscare using the contact details provided in this notice. Please note that this right is limited in healthcare settings. We are often required to retain records in line with legal, regulatory, and professional requirements, including the NHS Records Management Code of Practice. In these cases, we may not be able to delete your information.
Where we agree to erase information, we may retain a minimal record (such as your name and basic details) to ensure your preferences are respected and to prevent further unwanted processing.
We will respond to your request within one month, unless an extension is permitted by law. If we are unable to comply with your request, we will explain the reasons.

ACCESSING YOUR INFORMATION

You have the right to request access to the personal information Nimbuscare holds about you. This is known as a Subject Access Request (SAR).

You can request:

- A copy of the information we hold about you
- Details about how your information is used
- Information about who your data has been shared with, where appropriate

To make a request, you can contact Nimbuscare using the details provided in this notice.
To help us process your request efficiently, we may ask you to:

- Provide proof of your identity (for example, photographic ID or confirmation of personal details)
- Provide enough information to help us locate the records you require (such as dates, services accessed, or locations)

This is to ensure that we protect your information and only disclose it to the correct person.
We will normally respond to your request within one month of receiving sufficient information to process it. In some cases, where requests are complex or involve a large amount of information, we may extend this period by up to a further two months. If this happens, we will inform you and explain the reasons.

There is usually no charge for making a Subject Access Request. However, a reasonable fee may be charged in limited circumstances, for example where requests are excessive, repetitive, or manifestly unfounded.

In some situations, we may need to withhold or redact information. This may include:

- Information relating to other individuals (third-party confidentiality)
- Information that could cause serious harm to your or another person's physical or mental health
- Information that we are legally required or permitted to withhold

If we are unable to provide part or all of the information requested, we will explain the reasons where appropriate.

Where your information is held jointly with, or originates from, another organisation (such as your GP practice or a hospital), we may advise you to contact that organisation directly or coordinate a response with them.

If you would like information in a specific format (for example, electronic or paper copy), please let us know and we will do our best to accommodate your request.

CORRECTING YOUR INFORMATION

If you believe information, we hold is inaccurate or incomplete, please contact us.

Where your demographic details are maintained through your registered GP practice, we may ask you to contact your GP practice directly so the shared record can be updated correctly across systems.

THIRD PARTY INFORMATION IN YOUR RECORD

Sometimes we record information about third parties mentioned by you to us during any consultation or contained in letters we receive from other organisations. We are under an obligation to make sure we also protect that third party's rights as an individual and to ensure that references to them which may breach their rights to confidentiality, are removed before we send any information to any other party including yourself.

TELEPHONE CALLS, CCTV, AND WEBSITE USE

Nimbuscare may use systems such as call recording, CCTV, and website technologies to support the safe, effective, and secure delivery of our services.

TELEPHONE CALL RECORDING

We may record telephone calls for purposes including:

- Ensuring patient safety and quality of care
- Training and development of staff
- Investigating incidents, complaints, or concerns
- Verifying information where there is a dispute
- Supporting service monitoring and improvement

Call recordings are only accessed by authorised staff where there is a legitimate need to do so and are retained in line with our records management policies.

CCTV

CCTV may be in operation at some Nimbuscare sites. This is used for:

- The safety and security of patients, staff, and visitors
- The prevention and detection of crime
- The protection of property and assets

CCTV is positioned in appropriate areas (for example, entrances, exits, and communal areas) and is not used in private areas such as clinical consultation rooms.

Images are securely stored and only accessed by authorised personnel where necessary. Nimbuscare will ensure footage is not retained for more than 30 days, unless it is required for evidential purposes in legal or other investigation proceedings, once the image retention period has expired, the footage itself is automatically erased.

Viewing of these digital images is controlled by Nimbuscare in accordance with the CCTV Policy, please use the contact us page on our website to request a copy.

WEBSITE AND ONLINE SERVICES

When you use our website or online services, we may collect limited information to:

- Ensure the website functions correctly
- Improve user experience
- Support service access and communication
- Monitor website performance and usage

This may include the use of cookies or similar technologies. Where required, you will be given information about how these are used and choices about managing your preferences.

Our website uses cookies. Please see our Cookies Policy for more information.

This privacy notice applies to Nimbuscare services. If you access external websites via links, their own privacy notices will apply.

LAWFUL AND PROPORTIONATE USE

All use of call recording, CCTV, and website technologies is carried out in line with data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Nimbuscare ensures that:

- The use of these systems is necessary and proportionate
- Individuals are informed through appropriate signage or notices
- Access to recordings and data is restricted to authorised personnel
- Appropriate retention and deletion processes are in place

Separate, more detailed policies apply to specific systems, including cookies, CCTV, and telephone recording.

CONTACTING YOU

Nimbuscare may contact you by telephone, SMS, email, letter, or other approved methods in connection with your care, appointments, services, follow-up, or relevant service communications.

It is important that you tell your GP practice or the relevant Nimbuscare service if your contact details change.

CONTACT US

If you have questions about this privacy notice or how your information is used, please contact Nimbuscare:

Email: Nimbuscare.feedback@nhs.net

Telephone: 01904 943690

Postal address:

Nimbuscare Ltd

Head Office
Gateway 1,
Holgate Park Drive,
Holgate,
York,
YO26 4GG

Information Governance Leads: Zoe Weeks and Jennifer Butcher

Data Protection Officer: Barry Jackson N3I

Caldicott Guardian: Dr Daniel Kimberling

COMPLAINTS

If you are unhappy with any element of our data processing methods, please contact the Governance and Quality Compliance Team in the first instance.

Email: Nimbuscare.feedback@nhs.net
01904 943690

If you feel that we have not addressed your concern appropriately, you have the right to lodge a complaint with the Information Commissioner's Office (ICO).

The ICO can be contacted on https://ico.org.uk and select "Raising a concern" or telephone: 0303 123 1113.

The ICO is the regulator for data protection and offers independent advice and guidance on the law

If you are happy for your data to be used for the purposes described in this privacy notice, then you do not need to do anything. If you have any concerns about how your data is shared, then please contact Nimbuscare.

CHANGES TO THIS NOTICE

We may update this privacy notice from time to time to reflect changes in our services, systems, legal requirements, or how we use information.
The latest version will always be available on our website

APPENDIX 1 SERVICES AND CARE SETTINGS

Service Category	Description	Typical Data Used
Urgent and Same Day Care	Assessment and treatment for patients requiring urgent, non-emergency care	Personal details, presenting symptoms, clinical assessments, referral information
Out of Hours Services	Healthcare services provided outside normal GP practice hours	Personal details, clinical history, consultation notes, care plans
Frailty and Integrated Neighbourhood Services	Proactive, coordinated care for patients with complex or long-term needs	Health and social care information, risk assessments, care plans, MDT discussion notes
Diagnostics and Community Diagnostic Centres (CDC)	Access to diagnostic testing and investigations to support clinical decision-making	Personal details, referral information, test requests, results
Health Checks	Preventative health assessments and screening programmes	Personal details, lifestyle information, clinical measurements, screening outcomes
Extended Access	Additional GP and primary care appointments outside core hours	Personal details, appointment information, consultation records
Asylum Health Services	Healthcare services tailored to the needs of asylum seekers and vulnerable populations	Personal details, health history, vaccination records, safeguarding information where relevant
Private Services	Non-NHS services provided by Nimbuscare	Personal details, service-specific clinical or administrative information
Practice Support	Support services provided to GP practices to enable safe and effective care delivery	Limited patient data where required, operational and service-level information
Transport and Support Services	Non-clinical services supporting patient care and service delivery	Personal details, appointment and location information, accessibility needs
Medicines Management and Optimisation	Review and optimisation of medications to ensure safe, effective, and appropriate treatment, including quality improvement initiatives such as deprescribing	Medication records, clinical history, diagnoses, risk factors, prescribing data, care plans
Resilience Hub (Mental Health Support)	Mental health and wellbeing support service, where patients may be identified through case finding within GP practices and referred via social prescribing pathways	Personal details (including National Insurance number where required for eligibility, funding, or reporting purposes), referral information, mental health and wellbeing information, risk assessments, care plans, and interaction records.

APPENDIX 2: DIGITAL SYSTEMS AND PROCESSORS

Nimbuscare maintains a live schedule of digital systems and suppliers. The systems listed above may change over time, and all are subject to appropriate data protection, security, and contractual controls.

System / Supplier	Purpose	Type of Information Used	Nimbuscare Role	Notes
Ombea	Patient feedback and experience surveys	Survey responses, may include limited identifiable data	Controller	Used to gather service feedback and improve care
Vatix	Incident reporting, lone worker safety, and risk management	Staff data and limited patient-related data where relevant	Controller	Supports staff safety and incident management
Yorkshire Health and Care Record (YHCR) / shared record tools	Shared care record across organisations	Identifiable health and care information	Joint Controller	Supports direct care and system-wide information sharing
RSS / iRefer / other referral portals	Referral management and coordination	Patient identifiers, referral details, clinical information	Controller / Processor	Role varies depending on service model
X-on	Telephony and call handling systems	Call recordings, contact details, call metadata	Controller	Used for communication, training, and quality assurance
Kynoby	Clinical documentation and care planning tools	Clinical notes and patient care information	Controller	Used within specific services where deployed
Calendly	Appointment booking and scheduling	Name, contact details, appointment information	Controller	Used to manage bookings and availability
MiiCare	Remote monitoring and care technology	Health, wellbeing, and monitoring data	Controller / Joint Controller	Role depends on service model
Heidi	Clinical documentation support / digital scribing	Clinical notes and consultation information	Controller	Subject to governance controls and clinical oversight
Pocketalk	Translation and communication support	Spoken language data (not routinely stored)	Controller	Supports communication with patients
TytoCare	Remote examination and diagnostic device	Clinical observations, images, and patient identifiers	Controller	Used for remote clinical assessment
SystmOne	Clinical record system	Full patient health record, identifiers, clinical data	Joint Controller	Primary system for direct care and shared records

PharmRefer (Pharmacy First system)	Pharmacy referral and triage	Patient identifiers, symptoms, referral details	Controller / Joint Controller	Used to refer patients to community pharmacies
SharePoint	Document management and collaboration	Documents, administrative and limited patient data where appropriate	Controller	Used for internal governance and document storage
PeopleHR	Workforce and HR system	Staff personal data, employment records	Controller	Used for workforce management
Sign Solutions / Interpreter services	Interpretation and accessibility support	Patient identifiers, communication needs	Controller	Used to support accessible care delivery
EPaCCS Summary Record (Black Pear)	End of life care coordination and shared summary record	Key clinical information, care preferences, advance decisions, patient identifiers	Joint Controller	Provides accessible summary information to professionals involved in end of life care
PCMIS (Patient Case Management Information System)	Case management, clinical documentation, and service reporting	Patient identifiers, clinical notes, assessments, care plans, referral and outcome data	Controller	Used to support clinical services, case management, and performance reporting within the Resilience hub

APPENDIX 3: PARTNER ORGANISATIONS AND SHARING CONTEXTS

Sharing Context	Description	Examples of Organisations / Services
Direct care and shared care	Sharing information to provide safe, effective, and coordinated care between professionals involved in your treatment	GP practices, NHS Trusts, community services, shared care record systems
Neighbourhood working and integrated teams	Collaborative working across services to coordinate care, support MDTs, and deliver proactive and preventative care	Primary Care Networks, Integrated Neighbourhood Teams, frailty services, UCR, virtual wards, mental health teams
Community pharmacy and Pharmacy First	Referral and information sharing with community pharmacies to provide timely treatment and advice where appropriate	Community pharmacies, Pharmacy First referral systems (e.g. PharmRefer)
Research and innovation partners	Use and sharing of data for approved research, service evaluation, and innovation to improve care and outcomes	NHS organisations, universities, research bodies, approved partners
Support services and logistics	Sharing information to enable operational delivery of services and patient support	Patient transport providers, interpretation services, digital platforms, telephony systems, logistics providers
National and regional NHS bodies	Sharing information for commissioning, planning, oversight, national systems, and statutory reporting	NHS England, Integrated Care Boards (ICBs), NHS Digital / national data services