

PEOPLE
INFORMATION
COMPLIANCE
QUALITY
TRUST
SAFETY
BETTER CARE



WHERE YOUR FUTURE BEGINS

PRIVACY NOTICE & YOUR INFORMATION RIGHTS



HOW WE
USE YOUR
INFORMATION



KEEPING
YOUR DATA
SAFE



YOUR
INFORMATION
RIGHTS



SHARING
INFORMATION
RESPONSIBLY



GET IN
TOUCH

*Your information. Your rights.
Our commitment.*

RESPECT
TRANSPARENCY
CONFIDENTIALITY
ACCOUNTABILITY
BETTER CARE



PEOPLE FIRST.
INFORMATION SECURE.
A BRIGHTER TOMORROW.



PRIVACY NOTICE & YOUR INFORMATION RIGHTS

Public Website Publication Copy

Organisation	OMRA Ltd	Website	www.omra.healthcare
Data Protection Officer	Kristina Merto	DPO contact	tina.merto@omra.agency
Contract Manager	Melanie Yabut	Approved by	Dr Mallikarjunagouda Bharamgoudar, Director
Effective date	10 September 2026	Last updated	11 September 2026
Version	1.0	Review	At least annually and following material change

1. Privacy at OMRA

OMRA Ltd provides and supports clinical insourcing and associated healthcare services. We are committed to handling personal information lawfully, fairly, transparently and securely. This notice explains the personal information we may use, why we use it, where it comes from, who we may share it with, how long we keep it and the rights available to individuals.

For some processing, OMRA determines the purposes and means of processing and acts as a data controller. In some NHS or Relevant Authority service arrangements, the Relevant Authority may be the controller of the clinical record and OMRA may process information under the contractual and information-governance arrangements agreed for that service. Where another organisation is responsible for your clinical record, its privacy notice should also be read alongside this notice.

2. Information we may use

- identity and contact information, including name, address, telephone number, email address and other identifiers where relevant;
- patient identifiers, referral, appointment, waiting-list and pathway information;
- clinical, treatment, diagnostic, outcome, discharge and follow-up information where required for authorised healthcare delivery;
- special category information, including health information and other sensitive information where necessary and lawful;
- workforce and recruitment information, including professional registration, credentialing, references, DBS/compliance, training and occupational information;
- rota, availability, attendance, deployment and service-delivery information;
- financial, invoicing, payroll, payment and supplier information;
- incident, complaint, safeguarding, governance, audit and correspondence information; and
- technical, access, device, security and audit-log information generated through authorised systems.

3. Where information comes from

Depending on your relationship with OMRA and the service concerned, information may come directly from you or from a Relevant Authority or NHS organisation, authorised healthcare professionals, Apera Ltd or another authorised delivery partner, professional or regulatory bodies, referees, recruitment and screening providers including CRB Online where applicable, suppliers, or other lawful and authorised sources. Where information is obtained from another source, OMRA will provide or make available the relevant privacy information within the period required by data protection law, unless an applicable exemption applies.

4. Why we use personal information

- to coordinate and deliver safe clinical and healthcare services and support continuity of care;
- to manage referrals, appointments, clinical pathways, treatment, discharge, results and follow-up where OMRA is authorised to do so;
- to recruit, credential, deploy, train, pay and manage healthcare professionals and other workers;
- to meet safeguarding, patient-safety, clinical-governance, quality and professional obligations;
- to investigate incidents, complaints and concerns and support audit, learning and improvement;
- to manage contracts, suppliers, invoices, payroll, payments, insurance and business administration;
- to maintain secure systems, access controls, cyber security, business continuity and fraud prevention;
- to comply with legal, regulatory, professional, NHS and contractual requirements; and
- to establish, exercise or defend legal claims where necessary.

5. Our lawful bases

OMRA documents the lawful basis for each processing activity in its information-governance records. The lawful basis depends on the purpose and circumstances. The following are the principal bases that may apply:

Processing purpose	Typical UK GDPR basis / condition
Healthcare service delivery and patient pathway support	Where OMRA acts under an NHS/Relevant Authority arrangement, processing is carried out under the applicable controller/processor arrangements. Where OMRA is a controller, an appropriate Article 6 basis is documented. Health information is processed only where an applicable Article 9 condition and UK law permit it, including healthcare-related conditions where relevant.
Recruitment, workforce administration and deployment	Article 6(1)(b) where necessary for a contract or steps before a contract; Article 6(1)(c) for legal obligations; and Article 6(1)(f) legitimate interests where appropriate. Special category information is processed only under an applicable Article 9 condition and Schedule 1 condition where required.
Finance, contracts and business administration	Article 6(1)(b), Article 6(1)(c) and/or Article 6(1)(f), depending on the activity.
Information security, fraud prevention, governance and service assurance	Article 6(1)(c) where a legal obligation applies and/or Article 6(1)(f) legitimate interests in protecting OMRA, individuals, systems, information and service delivery.
Consent-based activities	Article 6(1)(a) only where consent is the appropriate basis. Where OMRA relies on consent, it can be withdrawn at any time.

Where OMRA relies on legitimate interests, those interests may include safe and effective service administration, protecting information and systems, preventing fraud, maintaining business operations and managing professional or contractual relationships. OMRA considers the impact on individuals before relying on this basis.

6. Who we may share information with

We share personal information only where necessary, lawful and appropriately protected. Depending on the circumstances, recipients may include:

- the Relevant Authority or NHS organisation commissioning, hosting or responsible for the service;
- authorised healthcare professionals and organisations involved in the individual's care or pathway;
- Apera Ltd and other authorised delivery partners where they are involved in the commissioned service;
- professional, regulatory, safeguarding or statutory bodies where appropriate;
- recruitment, screening and compliance providers, including CRB Online where applicable;
- IT, cyber security, secure hosting, communications and other technology service providers;
- payroll, accounting, banking, insurance and professional advisers; and
- public authorities, law enforcement, courts or regulators where disclosure is required or permitted by law.

Where another organisation processes personal information on OMRA's behalf, OMRA requires appropriate contractual and security arrangements proportionate to the service and risk.

7. International processing

Where personal information is transferred or made accessible outside the United Kingdom, OMRA will ensure that the transfer is lawful and that an appropriate transfer mechanism and safeguards are in place where required. Depending on the destination and circumstances, this may include UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to approved standard contractual clauses, or another lawful mechanism. Information about applicable safeguards can be requested from the Data Protection Officer.

8. How long we keep information

OMRA keeps personal information only for as long as necessary for the purpose for which it is used and in accordance with applicable legal, NHS, professional, contractual and organisational retention requirements. Where patient information forms part of a Relevant Authority's clinical record, the applicable retention arrangements of that Authority apply to that clinical record. OMRA's own records are retained according to the relevant retention category and legal or contractual requirement, after which information is securely deleted, destroyed or anonymised where appropriate.

9. How we protect information

OMRA uses proportionate technical and organisational measures to protect personal information. These include role-based and least-privilege access where available, strong authentication and multi-factor authentication where appropriate, secure configuration and patching, endpoint and cyber security controls, secure communications, confidentiality requirements, workforce training, supplier assurance, security monitoring, incident management, business continuity and controlled disposal.

10. If you do not provide information

Some personal information is necessary for OMRA to provide or administer a service, assess suitability for a role, meet legal or contractual requirements, process payment or maintain safe and secure operations. Where information is required and is not provided, OMRA may be unable to complete the relevant process or provide the requested service or engagement. For patient care, any implications will be managed with the Relevant Authority or healthcare team responsible for the service, taking account of patient safety and applicable legal requirements.

11. Automated decision-making

OMRA does not currently make solely automated decisions about patients or workforce members that produce legal or similarly significant effects. If such processing is introduced, OMRA will assess it before use and provide meaningful information about the logic involved, the significance and expected consequences, and the safeguards and rights available to individuals.

12. Your information rights

Data protection law gives individuals rights in relation to personal information. The availability of a particular right can depend on the lawful basis and circumstances of the processing.

Right	What this means
Right to be informed	Receive clear information about how your personal information is collected and used.
Right of access	Request a copy of personal information held about you, subject to applicable legal provisions.
Right to rectification	Ask for inaccurate personal information to be corrected and incomplete information completed where appropriate.
Right to erasure	Ask for deletion where the right applies. This is not an absolute right and may not apply where information must lawfully be retained.
Right to restriction	Request restriction of processing in circumstances provided by data protection law.
Right to data portability	Receive certain information in a structured, commonly used and machine-readable format where the legal conditions apply.
Right to object	Object to certain processing. Where the law provides an absolute right to object, OMRA will respect it.
Automated decision-making rights	Receive appropriate safeguards where solely automated decision-making with legal or similarly significant effects is used.
Withdraw consent	Where OMRA relies on consent, withdraw it at any time. This does not affect processing that was lawful before withdrawal.
Right to complain	Raise a concern with OMRA and complain to the Information Commissioner's Office if you are dissatisfied with how your information has been handled.

YOUR RIGHT TO OBJECT: Where OMRA relies on legitimate interests, or another basis that gives you a right to object, you may object to the processing. OMRA will consider your objection in accordance with data protection law.

13. How to exercise your rights or ask a privacy question

For privacy questions, rights requests or concerns, contact OMRA's Data Protection Officer:

Data Protection Officer	Kristina Merto
Email	tina.merto@omra.agency
Organisation	OMRA Ltd
Website	www.omra.healthcare

OMRA may need to verify your identity before disclosing, correcting or deleting personal information. Requests are handled within the applicable statutory timescales and subject to any lawful exemptions or restrictions.

14. Complaints

We encourage you to contact OMRA first so that we can try to resolve your concern. You also have the right to complain to the Information Commissioner's Office (ICO).

Information Commissioner's Office	Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Telephone	0303 123 1113
Website	www.ico.org.uk

15. Patient privacy information

If you receive a service delivered by OMRA, authorised OMRA and/or delivery-partner healthcare professionals may need to access and record information about you within systems and processes agreed with the NHS organisation or Relevant Authority responsible for your service. Only information necessary for authorised care and related purposes should be used. This may include patient safety, clinical governance, service quality, pathway administration and authorised contract assurance.

Patient information may be shared with the organisation responsible for your care, authorised healthcare professionals and other organisations involved in your care, or where sharing is otherwise required or permitted by law. Where the Relevant Authority is the controller of your clinical record, its privacy information explains the primary arrangements for that record.

16. Printed and accessible copies

A printed copy of this notice or relevant patient privacy information can be requested. Where appropriate to the service, printed information may also be available at reception, waiting areas or clinic locations, included with patient information, or provided by staff.

If you need privacy information in another accessible format, OMRA will take reasonable steps to provide an appropriate version. Depending on individual need, this may include large print, easy-read style information, an accessible electronic copy, translated information or other reasonable communication support.

17. When we collect information from you

Where practicable, OMRA provides or signposts privacy information at the point personal information is collected. Online forms and electronic collection processes should direct individuals to the relevant privacy information. Recruitment, workforce and other collection processes provide or signpost the applicable information during collection.

18. Changes to this notice

OMRA reviews this notice at least annually and whenever a material change occurs in its services, processing purposes, information flows, recipients, technology, international transfers or legal requirements. Where OMRA intends to use existing personal information for a new purpose, it will review the transparency information and provide any additional information required before the new processing begins.

19. Governance

This Privacy Notice was originally reviewed on 10 September 2026 by Justin Jacoba, Information Officer, with operational review by Melanie Yabut, Contract Manager, and approved by Dr Mallikarjunagouda Bharamgoudar, Director. Version 2.0 was updated on 11 September 2026 to strengthen transparency information, reflect OMRA's designated Data Protection Officer and provide fuller information on lawful bases, international transfers, individual rights and complaints.