PRIVACY NOTICE

Ocala Healthcare is committed to protecting the privacy and security of your personal information.

This privacy notice explains how we collect, use, share, and protect your personal data in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Data Controller

Ocala Healthcare
Unit 9 Wharfside House, Prentice Road, Stowmarket, IP14 1RD
01473 941 211

Types of Personal Data Collected

We may collect and process the following categories of personal data:

- Personal identification information (e.g., name, date of birth, gender)
- Contact information (e.g., address, phone number, email address)
- Health and medical information (e.g., medical history, medication details, allergies)
- Emergency contact details
- Financial information (e.g., payment details for billing purposes)

Purposes of Processing

We collect and process your personal data for the following purposes:

- Providing care and support services tailored to your needs
- Managing and scheduling appointments
- Communicating with you and your authorised representatives
- Processing payments and managing billing
- Complying with legal obligations and regulatory requirements
- Ensuring the health, safety, and well-being of service users and staff
- Conducting research and quality improvement activities (in an anonymised and aggregated format)

Lawful Basis for Processing

We rely on the following lawful bases for processing your personal data:

- Contractual necessity: Processing necessary for the performance of a contract with you or to take steps at your request prior to entering into a contract.
- Legal obligations: Processing necessary to comply with our legal obligations, such as record-keeping requirements and safeguarding obligations.
- Vital interests: Processing necessary to protect your vital interests or those of another individual in emergency situations.
- Legitimate interests: Processing necessary for our legitimate interests, such as providing quality care, managing our services efficiently, and improving our operations. We ensure that your rights and freedoms are not overridden.

Data Sharing

We may share your personal data with the following categories of recipients, as required and permitted by law:

- Healthcare professionals and providers involved in your care
- Regulatory authorities, government agencies, and professional bodies as mandated by law
- Third-party service providers who assist in the delivery of our services (e.g., IT providers, payment processors)
- Third-party research organisations in an anonymised and aggregated format

International Transfers

In certain circumstances, we may need to transfer your personal data outside of the European Economic Area (EEA). We will ensure appropriate safeguards are in place to protect your data in accordance with applicable data protection laws.

Data Retention

We will retain your personal data for as long as necessary to fulfill the purposes outlined in this privacy notice or as required by law. We have implemented appropriate retention periods and procedures to ensure the secure disposal of personal data when no longer needed.

Your Rights

You have the following rights regarding your personal data:

- The right to access: You can request a copy of the personal data we hold about you.
- The right to rectification: You can request the correction of inaccurate or incomplete personal data.
- The right to erasure: You can request the deletion of your personal data in certain circumstances.
- The right to restrict processing: You can request the limitation of the processing of your personal data in certain circumstances.
- The right to data portability: You can request the transfer of your personal data to another organisation.
- The right to object: You can object to the processing of your personal data in certain circumstances.
- The right to lodge a complaint: If you believe your data protection rights have been violated, you have the right to lodge a complaint with the Information Commissioner's Office (ICO) or another supervisory authority.

Security Arrangements for Personal Data

At Ocala Healthcare, the security and protection of your personal data are of utmost importance to us. We have implemented robust security measures to ensure the confidentiality, integrity, and availability of the personal data we collect, process, and store. This section outlines the security arrangements we have in place for the personal data stored on Office 365 SharePoint.

Firewalls: We have implemented industry-standard firewalls to fortify our Office 365 SharePoint environment. These firewalls act as a shield, preventing unauthorised access and unauthorised network traffic from breaching our systems. Our firewall setup adds an extra layer of defence against external threats, ensuring the safety of your personal data.

Encryption: All personal data stored on Office 365 SharePoint is protected through encryption measures both in transit and at rest. During the transmission of data between your device and our SharePoint servers, we employ Transport Layer Security (TLS) encryption. This advanced encryption protocol guarantees secure data transmission and prevents unauthorised interception. Moreover, personal data residing within the SharePoint platform is encrypted at rest. This means that even if physical storage media were to be compromised, your personal data would remain inaccessible to unauthorised individuals.

Two-Factor Authentication (2FA): To heighten the security of your personal data, we have implemented a robust two-factor authentication mechanism. This security feature requires users to provide two forms of verification, typically a password and a unique verification code sent to a registered mobile device. By incorporating 2FA, we significantly reduce the risk of unauthorised access to your personal data, even if your password were to be compromised.

Rest assured that we continually review and update our security arrangements to align with industry best practices and stay ahead of emerging threats. Our commitment to safeguarding your personal data remains unwavering.

If you have any concerns or queries regarding the security of your personal data, please reach out to our dedicated Data Protection Officer.

ICO Contact Information

To make a complaint or contact the Information Commissioner's Office, you can call 0303 123 1113.

Alternatively, find more information on their website. https://ico.org.uk

Contact Us

If you have any questions or concerns regarding the processing of your personal data or would like to exercise your rights, please contact our Data Protection Officer at adam@ocalahealthcare.co.uk