Cortera Privacy Notice

Here at The Cortera Group, your privacy is important to us, and we are committed to protecting and safeguarding your data protection rights. This privacy notice lets you know what happens to any personal data that you give to us as well as any information that we may collect from you or information, we may receive from other organisations.

The Cortera Group comprises the following companies:

- Ascenti Health Limited
- Ascenti Physio Limited
- Advo Health Limited
- Six Physio Limited

This privacy notice covers the activities undertaken by Ascenti Health and Ascenti Physio **only**. Separate privacy notices are available for the other companies within the group.

This privacy notice explains:

- Who we are and the laws under which we are governed.
- What information we collect.
- How we use your personal information
- How we lawfully use your personal information.
- Who we may share you information with, including for safeguarding purposes.
- How we keep your personal information safe.
- Your individual data rights.
- How long we retain your personal information for.
- How to raise an objection/complaint.
- Contact information for our Data Protection Officer and the Information Commissioner's Office

For applicable Data Protection legislation, including the UK GDPR and the Data Protection Act 2018, Ascenti Physio is a data controller, registered with the Information Commissioner's Office with a registration number of **Z2452913.**

Ascenti Health is also a data controller registered with the Information Commissioner's Office with a registration number of **Z7390990.**

What information do we collect?

We collect personal information about you, which includes name, address, telephone number, email address, date of birth, next of kin information, NHS number etc, IP address. This enables us to provide the appropriate treatment for you.

We will also collect sensitive confidential information known as **"special category personal data,"** in the form of health information, religious beliefs, ethnicity, sexuality, disability status, pregnancy status, biometric data (if applicable) etc. and we may also receive this information about you from other health providers or third parties.

Payment information is required for those who will be responsible for paying for their own appointments and treatment, but the financial information such as credit/debit card details you provide is not stored by Cortera, as we use a third-party payment provider to provide secure transactions and to limit the financial information we store.

How do we use your information?

If you make an enquiry to access our services, we will use your data to respond to your enquiry. We will also use your data to send you service-related information or ask you to provide feedback.

As a healthcare organisation we maintain records about your health and any treatment or care you have received previously. These records help to provide you with the best possible healthcare and treatment.

The Cortera Group is a provider of healthcare services, and we use digital systems to help us to deliver the most efficient services to you and make records of your assessment and any treatment you agree to. We use a combination of technical and organisational measures to ensure that your information is kept confidential and secure.

The health records we store includes the following information:

- Details about you, such as your name, date of birth, address, contact telephone number, email address, as well as details of anybody else connected with your care such as a carer or legal representative and their emergency contact details.
- Details relating to any contact you have had with us you, including phone calls, appointments attended, any missed appointments etc.
- Clinical notes and reports about your health, including any past or present symptoms, diagnosed conditions, medications you may take, allergies you have etc.
- Details of your assessment, including any questionnaires you are asked to complete, including assessments tools used to evaluate your condition.
- Results of investigations such as blood tests, x-rays etc
- Relevant information from other health professionals, relatives or those who care for you.

We only use the information you provide us with to help deliver the most effective services to you and do not use it for any other purposes unless required to do so by law, or with your explicit consent. Some of your information may be used for clinical audit purposes to monitor the quality of the services we provide. We use a dedicated platform to manage customer relationships, communications, enquiries and marketing activities to enable effective communications and delivery of services.

Cortera Health Group

Use of Heidi AI for Clinical Note Keeping

To help our clinicians create clear and accurate notes after your appointment, we use a secure tool called Heidi AI. This tool helps turn the clinician's written or spoken information into a draft note. It is simply an administrative aid, and it does not make any decisions about your care. A clinician always reviews and finalises the notes before they become part of your health record.

Why we use it

Using Heidi AI helps us:

- create accurate notes while the information is still fresh
- reduce admin time, allowing clinicians to spend more time focused on your care
- ensure your record is completed quickly and clearly
- How your information stays safe

Your data is kept secure at all times. We use Heidi AI within a controlled environment that meets our data protection and clinical safety standards. Importantly, your information is not used to train the AI system, and it is not shared for any other purpose.

Your rights

You have the same rights over information typed with the help of Heidi AI as with any part of your health record. This includes the right to:

- see your record
- ask us to correct inaccurate information
- raise any questions about how your data is used

How do we lawfully use your information?

We need your personal information to provide you with healthcare services and to enable us to use this information, we must apply a lawful basis, as required under the UK GDPR/DPA18. The following lawful bases (found in Article 6 of the UK GDPR) will be the most applicable ones when the Ascenti Group lawfully processes your information:

- **Consent** – We would obtain freely given, specific, unambiguous, and explicit consent to process your personal data for certain purposes.
- **Contract** – The processing is necessary for the performance of a contract you are party to or take steps at your request before entering a contract.
- **Legal Obligation** – The processing is necessary for us to comply with the law.
- **Vital Interests** – The processing is necessary to protect someone's life, for example providing your information to the emergency services in the event of an emergency.
- **Public Interest** – The processing is necessary to perform a task in the public interest or for official functions and the task or function has a clear basis in law.
- **Legitimate interests** – The processing is necessary to meet our legitimate interests.

Processing your health data

To process your health data, additional safeguards are required due to the sensitivity of the data, so we must apply the appropriate lawful exemption; a list of these exemptions can be found in Article 9 of the UK GDPR. The following exemption is applied to allow us to process your health data:

Article 9 (2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems.

Also, if there is a safeguarding concern raised with us then information may be shared to protect the adult or child whose safety is a concern to the healthcare professionals.

We have set out in the table below the lawful bases that we rely on when we use your data:

Purpose	Article 6 condition	Article 9 condition
All Patients		
Cooperate with regulators, e.g. the Care Quality Commission	Article 6(1)(e) – public task Article 6(1)(c) – compliance with a legal obligation	Article 9(2)(g) – substantial public interest
Compliance with legal obligations, e.g. a court order requiring us to release information	Article 6(1)(c) – compliance with a legal obligation	Article 9(2)(f) – establishment, exercise, or defence of legal claims Article 9(2)(g) – substantial public interest
Dealing with disputes, for example if you make a legal claim/complaint against us	Article 6(1)(f) – legitimate interests (we have a legitimate interest in being able to deal with disputes and legal claims)	Article 9(2)(f) – establishment, exercise, or defence of legal claims
Dealing with any risk to public health	Article 6(1)(e) - public task Article 6(1)(c) – compliance with a legal obligation	Article 9(2)(h) – healthcare and social care purposes Article 9(2)(i) – public health

Purpose	Article 6 condition	Article 9 condition
NHS Patients		
Providing you with our services	Article 6(1)(e) - public task Article 6(1)(c) – legal obligation	Article 9(2)(h) – healthcare and social care purposes
Helping to maintain the quality of and improve our services	Article 6(1)(e) - public task Article 6(1)(c) – legal obligation	Article 9(2)(h) – healthcare and social care purposes
Providing assessment report and other clinical information back to your NHS GP surgery	Article 6(1)(e) - public task Article 6(1)(c) – legal obligation	Article 9(2)(h) – healthcare and social care purposes
Helping other organisations delivering NHS or social care to provide you with services.	Article 6(1)(e) - public task/duty of data controller	Article 9(2)(h) – healthcare and social care purposes

Purpose	Article 6 condition	Purpose
Letting you know more about our services and offers, including those from relevant third parties	Article 6(1)(a) - consent	Article 9(2)(a) – consent
Planning and research purposes	Article 6(1)(a) - consent	Article 9(2)(a) – consent

Purpose	Article 6 condition	Purpose
Private Patients		
Providing you with our services	Article 6(1)(b) – performance of a contract Article 6(1) (f) – legitimate interests	Article 9(2)(h) – healthcare and social care purposes
Providing assessment report and other clinical information back to your NHS GP surgery	Article 6(1)(e) – duty of data controller Article 6(1)(c) – legal obligation	Article 9(2)(h) – healthcare and social care purposes
Helping to maintain the quality of and improve our services	Article 6(1)(f) – legitimate interests (we have a legitimate interest in maintaining and improving the quality of our services)	Article 9(2)(h) – healthcare and social care purposes
Obtaining payment from you for our services	Article 6(1)(b) – performance of a contract	No special category data used
Letting you know more about our services and offers, including those from relevant third parties	Article 6(1)(a) - consent	Article 9(2)(a) – consent
Planning and research purposes	Article 6(1)(a) - consent	Article 9(2)(a) – consent

Who do we share information with?

As stated in this Privacy Notice, we may have to share your information, subject to strict contracts and agreements, with any of the following organisations:

- Other members of The Cortera Group
- GP Practices
- Scan diagnostic providers to facilitate any x-rays, MRI scans, CT scans etc as required to aid your diagnostics.
- Other private sector providers, under contract and to meet lawful obligations.
- Solicitors, insurers, or other instructing party
- Emergency services, if required to facilitate welfare/safeguarding checks

- Police & Judicial Services
- Regulators such as the Care Quality Commission

You will be informed who your data will be shared with and in some cases asked for consent for this to happen when this is required.

There are times when we may be required by law to share your information without your consent, for example:

Where we have an overarching lawful basis that allows us to share, for example for your direct health care needs. This includes sharing information with your GP if you have been referred under Right to Choose or through a contract your local NHS provider hold with us. We are required to share information, including a copy of the assessment report, to update your GP on your referral, and this information is transmitted using encrypted email and is stored under strict security controls as part of your GP record.

- For private patients we are still required to share information with your GP if you have been diagnosed with a specific condition that must be recorded in your health record as it is imperative that your GP record includes this to safeguard you and ensure an accurate account is available to those involved in your direct care. If you have concerns about this, you are advised to speak directly with the clinician involved in your care.
- Where a serious crime, such as assault, is being investigated or where it could be prevented.
- Where a formal court order has been issued.
- Where there is a legal requirement.

The Cortera Group is committed to ensuring that when required to share personal information we will endeavour to share only the minimal amount of information as is necessary for the given purpose.

Safeguarding

The Cortera Group is dedicated to ensuring that the principles and duties of safeguarding adults and children are consistent and ethically and morally applied with the wellbeing of all patients being at the heart of what we do.

Our legal basis for processing information for safeguarding purposes, as stipulated in the UK GDPR is:

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 vested in the controller.

Article 6(1)(d) processing is necessary to protect the vital interests of the data subject or of another natural person.

For the processing of special categories data, the basis is:

Article 9(2)(b) – 'processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.

Categories of personal information when handling safeguarding issues

The personal information collected by The Cortera Group in the event of a safeguarding situation, will be minimised to include only the personal information that is necessary to handle the situation in the most

appropriate way. This may mean sharing basic demographic and contact information, as well as details of what the safeguarding concern is.

National Data Opt-Out

The National Data Opt-Out (NDOO) allows individuals to choose, in specified circumstances, if data from their health records is shared for healthcare research and planning. Although The Cortera Group is a private provider, we are required to comply with the National Data Opt-Out by having suitable policies, processes, and procedures in place. The service enables individuals to view or change their National Data Opt-Out choice at any time. This can be done:

- through the NHS App by clicking on "Your Health" and selecting "Choose if data from your health records is shared for research and planning"
- online via the NHS data matters page
- by phone, email or post via the manage your choice page

How do we keep your information safe?

We ensure all information you provide to us is stored securely and adhere to strict technical and organisational measures to protect your information. We will take all reasonable precautions to prevent the loss, misuse or alteration of information received.

All electronic records are stored on encrypted servers and devices, with up-to-date Antivirus and Firewall software applied. Unauthorised access to information is prevented by using restricted permission controls and multi-factor authentication.

We operate on a principle of minimal access, granting permissions only where necessary. Our patient management system uses role-based groups to ensure that only authorised staff can access patient files.

Formal electronic reports transmitted externally are protected using encryption and/or password protection.

Whilst face to face assessments form part of our service, there may be occasions where we use secure video conferencing tools which feature end-to-end encryption for online chat, visual-audio calls, visual-audio appointments to ensure confidentiality. We may record audio-visual calls and audio-visual appointments, but this would never be done without firstly obtaining your explicit consent.

Whilst we endeavour to keep our systems and communications protected against viruses, malware, and other harmful effects, we cannot bear responsibility for all communications not being virus or malware free.

Your individual data rights

As an individual you have the following rights in relation to your personal information:

Right to be informed – as a data controller, we are required to inform individuals when their personal information is collected and about the intended purposes behind the processing of that information. This privacy notice ensures as an organisation we satisfy this right. We will ensure we update this notice on a

regular basis to ensure you continue to be appropriately informed of how your personal information will be used.

Right to access your personal information - Everybody has the right to access their own personal information, as well as information relating to processing activities, and receive a copy of that information. This right is commonly referred to as a Data Subject Access Request (DSAR).

You can also make requests via the following methods:

By Post to the following address: providing detail on what information you are requesting.

Carnac House, Cams Hall Estate, Fareham, Hampshire PO16 8UZ

By sending an email to: SAR@Ascenti.co.uk
Verbally when engaged in a call 0330 678 0850

There is no fee for a Subject Access Request, and you will receive your information within one calendar month from the date of request. For complex requests we are entitled to apply an extension of a further 2 months, but you will be informed of this as soon as possible to manage your expectations. To validate any request for information we may need to obtain proof of identity and in the case of third-party requests, the required authority to act must be provided before we can disclose any personal information.

Please be mindful that when we release information to satisfy a Data Subject Access Request the information is for the personal use of the requestor only. It is not to be shared with anybody else and not to be used inappropriately, for example posting onto social media sites. Individuals can be subject to prosecution for posting information in the public domain as ruled by the High Court.

Right to rectification - The correction of personal data when incorrect, out of date or incomplete will be rectified by us without undue or excessive delay. If, however, such requests are linked to legally significant matters, such as confirming legal identity, we may require proof of any alleged inaccuracy before we are able to rectify the information held. Please ensure when consulting with us that we always have the correct contact details for you and be prepared to have personal information checked and verified at every appointment/telephone call. If you wish to make a request to rectify your personal information, please email SAR@Ascenti.co.uk

Right to erasure – Under Article 17 of the UK GDPR individuals have the right to have personal data erased or deleted. This is also known as the 'right to be forgotten.' The right is not absolute and only applies in certain circumstances, for example when your personal data is no longer necessary for the purpose for which it was originally collected or processed. If you wish to make a request to erase personal information, please email SAR@Ascenti.co.uk

Your erasure request can be instantly fulfilled in respect of live systems, but that the data will remain within the backup environment for a certain period until it is overwritten.

Right to restrict processing – Article 18 of the UK GDPR gives individuals the right to restrict the processing of their personal information in certain circumstances. This means that you can limit the way

that the organisation uses your information. This is an alternative to requesting the erasure of your information. If you wish to make a request to restrict the processing of personal data, please email **SAR@Ascenti.co.uk**

Right to data portability - Under UK GDPR, individuals have the right to data portability in situations where the personal information that they have provided to us is processed by automated means on the basis of consent, or where the personal information is necessary for the performance of a contract. Individuals are entitled to have their personal information transmitted directly from one data controller to another if it is technically feasible to do so. This means being in a structured, commonly used, and machine-readable format.

Right to object to processing - Individuals have the right to object to the processing of their personal information on grounds relating to their situation and to data processed for direct marketing purposes, however if we can demonstrate compelling legitimate grounds to process the information then processing can continue. If we did not process any personal information about you and your health care needs, it would be difficult for us to care for and treat you. If you wish to object to the processing of personal data, please email SAR@ascenti.co.uk.

Rights in relation to automated decision making and profiling - Automated individual decision-making is a decision made by automated means (i.e., a computer system) without any human intervention. If any of the processes we use rely on automated decision making, you do have the right to ask for a human to review any computer-generated decision at any point. We use automated tools within our Reach application to triage cases to our clinical professionals – all clinical decisions are made by humans, and we do not engage in any form of profiling.

The Ascenti Reach Application

If you have registered to use our Reach application, the information you provide, including your health data, will be reviewed by a qualified physiotherapist. Your physiotherapist will use this information to understand your needs, determine the most appropriate next steps in your care, and assign a bespoke treatment plan where necessary. We use digital tools to assist in this process, but all decisions about your care are made by a qualified clinician.

We also analyse aggregated and anonymised health data to help us evaluate and improve our clinical pathways and digital tools. This analysis never affects individual decisions about your care.

We require your consent to process your health data in this way. By clicking **'Continue'** within the Ascenti Reach app, you are providing your consent. You can withdraw your consent at any time by contacting us at reach@ascenti.co.uk If you do not consent, please click **'I'd like to contact someone'** within the app to speak with a member of our team and discuss alternative options.

How long do we keep your information for?

When storing your personal information, The Cortera Group ensures, as required under UK Data Protection legislation, that we keep your information for the required timeframes.

Deletion of Personal Data

We only keep your personal data, including health information, for as long as necessary to provide care, meet legal and regulatory requirements, and support clinical governance. When your data is no longer required, we will securely delete or anonymise it in accordance with our retention policies.

Deletion is carried out using appropriate technical and organisational measures. This may include securely removing data from our systems so that it cannot be recovered, permanently destroying records or storage media, or anonymising data so that you can no longer be identified.

Data held in backups is not routinely accessed and will be securely overwritten or deleted in line with our retention schedules.

Where we use third-party service providers, we require them to securely delete or return personal data once it is no longer needed, in line with contractual obligations.

In some cases, we may retain limited information for longer where we are required to do so by law or to establish, exercise, or defend legal claims. Access to such data will be strictly controlled.

Key Contacts/Complaints

Should you have any concerns about how your personal information is managed, please contact:

Data Protection Officer

If you wish to raise a data matter directly with the Cortera Group's Data Protection Officer, you can send an email to: dpo@ascenti.co.uk

If you have a complaint about anything else, please contact the Team using the below details:
Email: contact@ascenti.co.uk or alternatively use our contact form on our Cortera website

Lodging a complaint with the ICO

You also have the right to lodge a complaint with the UK's independent authority on data protection issues, if you are unhappy with the way your personal information has been processed. This regulatory authority is the Information Commissioner's Office, and you can contact them using the methods listed below:

Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel: 0303 123 1113
Website contact: https://ico.org.uk/