



Privacy Policy

Summary	Privacy policy covering all aspects of gathering, processing and sharing personal data within the company.
Author	Mark Edson
Target Audience	All company employees, representatives, service users and the general public.
Date Issued	22/05/2026
Approved by Directors	26 TH June 2026
Next Review Date	May 2027

Capmed Diagnostics discourages the retention of hard copies of policies and procedures. The company can only guarantee that the policy in the company website is the most up-to-date version. If, in exceptional circumstances, you need to print a policy off, it is only valid for 24 hours.

Version Control

Date	Author	Version	Page	Change / Reason for change
22/05/2025	Mark Edson	1.0		Original document created.

Contents

Contents	2
Introduction	4
Scope	4
Definitions	4
Roles and Responsibilities	5
Directors	5
Employees / Company Representatives	5
Patients / Service Users / Members of the public	6
Procedures and Processes	6
1. Contact Details	6
2. What information we collect, use and why	6
3. Data Protection Rights	8
4. Our lawful bases for the collection and use of your data	8
5. Where we get personal information from	10
6. How long we keep the information	10
7. Who we may share information with	12
National MRI Scan Ltd trading as Scan.com	12
Medichecks.com Ltd	12
Cloud Rx Ltd	12
8. Data Processors	13
Pathway Software UK (Ltd)	13
Stripe Payments UK Ltd	13
9. Others we may share personal information with	13
Compliance and Enforcement	13
1. Duty of Confidentiality	13

2. Contracts, Data Sharing Agreements and Service Level Agreements	14
3. Complaints	14
Related Policies	15

Introduction

This privacy policy tells you what to expect Capmed Diagnostics, herein referred to as the Company, to do with your personal information. The policy specifically outlines

- Company contact details.
- What information we collect, use, and why.
- Lawful bases and data protection rights.
- Where we get personal information from.
- How long we keep information.
- Who we share information with.
- How to complain.

Scope

The policy covers all data obtained, used and processed by the company from service users, carers or family members. It applies to all personal data processing carried out by the Company on personal data.

Definitions

Term	Definition
Consent	In relation to the processing of personal data relating to an individual, means freely give, specific, informed and unambiguous indication of the individuals wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of their personal data.
Data Controller	The organisation who decides why they are processing information and how personal data is handled and what their legal justification for doing this is.
Data Processors	Data processors act on behalf of the Data Controller. The Data Controller instructs the Data Processor to perform tasks on data for them.
Information Commissioners Office (ICO)	The UK supervisory authority responsible for regulating data protection and freedom of information compliance of organisations.
Organisation	A external legal entity that the Company has a relationship with (but no control over) to provide additional services or functionality that the Company is unable to provide itself.
Personal Data	Information that relations to an identified or identifiable living individual e.g a name or NHS Number. It should be considered if an individual could be indirectly identified by combining other data. Personal data does not include information relating to deceased individuals, or information regarding companies or public

	authorities (unless the company is a sole trade, and an individual can be identified)
Privacy Notice	Public document which explains to the individuals that you process data about what information you process about them, the purpose for which you process the data, details of who you share data with and why, and what rights they have over their data. This policy constitutes the Company privacy notice.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Retention	The length of time that records should be kept in line with statutory provisions or in line with the length of time an organisation deems the record to be useful.

Roles and Responsibilities

Directors

- Ensure they are aware of the content of the policy and update in compliance with any change in legislation.
- Communicate the policy to any company employees or representatives processing personal data within the scope of this policy.
- Check compliance with this policy and/or any subsequent data sharing agreements out into place as a result of this policy.
- Register the Company with the Information Commissioners Office and maintain accurate registration.
- Report any data breach to the correct authorities in line with current legislation.
- Ensure appropriate IT precautions have been taken to maintain data privacy and security.

Employees / Company Representatives

- Be aware of the content of this policy.
- Raise to the attention of the directors any non-compliance with this policy that risks the personal data held by the company.
- Process all data covered in the scope of this policy in compliance with policies and procedures outlined.
- Report any data breach as soon as they are aware to the directors.

Patients / Service Users / Members of the public

- Awareness of their rights within the context of this policy to access any personal data held by the Company

Procedures and Processes

1. Contact Details

Any individual that has any concerns about data privacy and/or wishes to exercise their rights under current legislation should contact the company at the earliest opportunity.

The quickest method to contact the Company is via email. However, the Company seeks to provide as many methods of contact as possible and can therefore be contacted in relation to data privacy by the following methods:

Email: privacy@capmeddiagnostics.co.uk

Tel:

Mail: 61 Bridge Street, Kington, HR5 3DJ

The Company commits to providing up to date contact details for service users in relation to the Privacy policy on it's website at www.capmeddiagnostics.co.uk.

2. What information we collect, use and why

We collect or use the following information **to provide patient care, services, pharmaceutical products and other goods:**

- Name, address and contact details
- Gender
- Pronoun preferences
- Date of birth
- NHS/HSC/CHI number
- Hospital number
- Next of Kin details including any support networks
- Emergency contact details
- Health information (including medical conditions, allergies, medical requirements and medical history)
- Information about care needs (including disabilities, home conditions, medication and dietary requirements and general care provisions)
- Test results (including psychological evaluations, scans, bloods, x-rays, tissue tests and genetic tests)
- Payment details (including card or bank information for transfers and direct debits)
- Insurance policy details
- Call recordings

We also collect the following special category information **to provide patient care, services, pharmaceutical products and other goods**. This information is subject to additional protection due to its sensitive nature:

- Racial or ethnic origin
- Health information

We collect or use the following personal information **for patient app or portal functionality**:

- Names and contact details
- Addresses
- Medical history
- Payment details
- Account information, including registration details
- Information used for security purposes

We also collect the following special category information **for patient app or portal functionality**. This information is subject to additional protection due to its sensitive nature:

- Health information

We collect or use the following personal information for **dealing with queries, complaints or claims**:

- Names and contact details
- Addresses
- Payment details
- Account information
- Purchase or service history
- Call recordings
- Relevant information from previous investigations
- Customer or client accounts and records
- Information relating to health and safety (including incident investigation details and reports and accident book records)
- Correspondence

We also collect the following special category information **for dealing with queries, complaints or claims**. This information is subject to additional protection due to its sensitive nature:

- Health information

3. Data Protection Rights

Under UK data protection law, we must have a “lawful basis” for collecting and using your personal information. There is a list of possible lawful bases in the UK GDPR. You can find out more about lawful bases on the ICO’s website.

Which lawful basis we rely on may affect your data protection rights which are set out in brief below. You can find out more about your data protection rights and the exemptions which may apply on the ICO’s website:

- **Your right of access** - You have the right to ask us for copies of your personal information. You can request other information such as details about where we get personal information from and who we share personal information with. There are some exemptions which means you may not receive all the information you ask for. Read more about the right of access.
- **Your right to rectification** - You have the right to ask us to correct or delete personal information you think is inaccurate or incomplete. Read more about the right to rectification.
- **Your right to erasure** - You have the right to ask us to delete your personal information. Read more about the right to erasure.
- **Your right to restriction of processing** - You have the right to ask us to limit how we can use your personal information. Read more about the right to restriction of processing.
- **Your right to object to processing** - You have the right to object to the processing of your personal data. Read more about the right to object to processing.
- **Your right to data portability** - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you. Read more about the right to data portability.
- **Your right to withdraw consent** – When we use consent as our lawful basis you have the right to withdraw your consent at any time. Read more about the right to withdraw consent.

If you make a request, we must respond to you without undue delay and **in any event within one month**.

To make a data protection rights request, please contact us using the contact details within this this privacy notice.

4. Our lawful bases for the collection and use of your data

Our lawful bases for collecting or using personal information to provide **patient care, services, pharmaceutical products and other goods** are:

- **Consent** - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.

- **Contract** – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.
- **Legitimate interests** - we're collecting or using your information because it benefits you, our organisation or someone else, without causing an undue risk of harm to anyone. All of your data protection rights may apply, except the right to portability. Our legitimate interests are:
 - Information is collected to be able to signpost patients to alternative care pathways and/or providers, following use of services, to promote improvements in symptoms and/or overall physical and/or mental health based upon the findings of consultation and/or diagnostic testing.

For more information on our use of legitimate interests as a lawful basis you can contact us using the contact details set out above.

- **Vital interests** – collecting or using the information is needed when someone's physical or mental health or wellbeing is at urgent or serious risk. This includes an urgent need for life sustaining food, water, clothing or shelter. All of your data protection rights may apply, except the right to object and the right to portability.

Our lawful bases for collecting or using personal information for **patient app or portal functionality** are:

- **Consent** - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.
- **Contract** – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.
- **Vital interests** – collecting or using the information is needed when someone's physical or mental health or wellbeing is at urgent or serious risk. This includes an urgent need for life sustaining food, water, clothing or shelter. All of your data protection rights may apply, except the right to object and the right to portability.

Our lawful bases for collecting or using personal information for **dealing with queries, complaints or claims** are:

- **Consent** - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.
- **Contract** – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.
- **Vital interests** – collecting or using the information is needed when someone's physical or mental health or wellbeing is at urgent or serious risk. This includes an urgent need for life sustaining food, water, clothing or shelter. All of your data protection rights may apply, except the right to object and the right to portability.

5. Where we get personal information from.

- Directly from you
- Family members or carers
- Other health and care providers
- Insurance companies

6. How long we keep the information

The retention periods given in this policy are the minimum periods for which records must be retained for health and care purposes. In most cases, it will be appropriate to dispose of records once this period has expired, unless the records have been selected for permanent preservation.

If a situation arises where it is necessary to maintain specifically identified individual records, or group of records for longer than the stated minimum, where records contain personal data, the decision to retain must comply with UK GDPR.

Approval for continued retention beyond the periods laid out in this policy should be in exceptional circumstances only and written approval must be sought from the director, and a specific period set for further review.

Record Type	Category	Retention Period	Notes
Adult health records not covered by any other section in this schedule (includes medical illustration records such as x-rays and scans as well as video and other formats. Also includes care plans)	Care Record	8 Years	
Electronic Patient Record Systems	Care Record	8 Years (see notes)	Where the system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain, demonstrating the destruction, then the Code should be followed in the same way for digital as well as paper records with a log kept of destruction. If the EPR does not have this capacity, then once records reach the end of their retention period, they should be made inaccessible to system users upon decommissioning. The system, along with the audit trails, should be retained for the retention period of the last entry related to the schedule
Clinical Audit	Event and transaction record	5 Years	Five years from the year in which the audit was conducted. This includes the reports and data collection sheets/exercise. The data itself will usually be clinical so should be kept for the appropriate retention period, for example, data from adult health records would be kept for 8 years.

Clinical Diaries	Event and transaction record	2 Years	Two years after the year to which they relate. Diaries of clinical activity and visits must be written up and transferred to the main patient record. If the information is not transferred from the diary, so the only record of the event is in the diary, then this must be retained for eight years and reviewed. Some staff keep hardback diaries of their appointments or business meetings. If these contain no personal data, they can be disposed of after two years.
Equipment Maintenance Logs	Event and transaction record	11 Years	
Referrals: NOT ACCEPTED	Event and transaction record	2 Years	Retention begins from the date of rejection.
Recorded conversations: which may be needed later for clinical negligence or other legal purpose	Telephony systems and services	6 Years	Retention period runs from the date of the call and is intended to cover the Limitation Act 1980.
Recorded conversations: which form part of the health record	Telephony systems and services	8 Years	Treat as a Health Record
Company Contracts that do not form part of a health record. Including terms of business, supplier and customer contracts.	Corporate Records	6 Years	
Accounting Records: including Financial details, director reports and shareholder specifics	Corporate Records	6 Years	
Tax Records: including Invoices, revenue and expenditure.	Corporate Records	6 Years	
Employment Records: Including Payroll details and employee contracts	Corporate Records	6 Years	
Data Protection Records: including Personal data records and processing logs	Corporate Records	6 Years	
Health and Safety Records: including Incident logs and risk registers	Corporate Records	6 Years	
Policies, strategies and operating procedures, including business plans	Corporate Records	6 Years	Retention starts after the document is superseded.
Patient Complaints	Corporate Records	10 Years	From the end of the financial year in which the complaint was handled.
Incidents: Not Serious	Corporate Records	10 Years	
Incidents: Serious	Corporate Records	20 Years	
Patient Information Leaflets	Communication	6 Years	
Press Releases	Communication	6 Years	
Website	Communications	6 Years	Previous public facing pages should be saved prior to adjustment. Retention period begins from the date the page is no longer live.

For more information on how long we store your personal information or the criteria we use to determine this please contact us using the details provided above.

7. Who we may share information with

The Company may need to share information with other organisations that provide services in relation to an individual patient care pathway. For example, Phlebotomy testing as part of pre-assessment screening or additional diagnostic scanning to confirm that a capsule has left the patients body and is not retained.

The Company will not share any information for commercial gain with other organisations (outside of payment processing) and will only share the minimum amount of information required with the relevant organisation to enable a particular portion of the care pathway to be delivered.

National MRI Scan Ltd trading as Scan.com

The following information may be shared with the above for selected patients as part of the provision of imaging services for additional diagnostic scanning as part of the relevant patient pathway;

- Name, address and contact details
- Gender
- Pronoun preferences
- Date of birth
- NHS/HSC/CHI number
- Hospital number
- Health information (relevant allergies and medical requirements related to the provision of the required imaging service)
- Information about care needs (including any disabilities that need to be considered in the delivery of the imaging required)

Medichecks.com Ltd

The following information may be shared for selected patients in the provision of remote phlebotomy services for patients requiring blood testing as part of their pathway.

- Name, address and contact details
- Pronoun preferences
- Date of birth

Cloud Rx Ltd

The following information may be shared for selected patients in the provision of Pharmaceutical goods as part of the patients pathway;

- Name, address and contact details
- Gender
- Pronoun preferences

- Date of birth
- Health information (relevant allergies, current medication information that would be relevant to the provision of the prescribed medication)

8. Data Processors

Pathway Software UK (Ltd)

This data processor does the following activities for us:

- Manages our Electronic Patient Record System storing all patient information, treatment plans and correspondence.

Stripe Payments UK Ltd

This data processor does the following activities for us:

- Process all electronic payment information.

9. Others we may share personal information with

- Other health providers (eg GPs and consultants)
- Insurance companies, brokers and other intermediaries
- Organisations we need to share information with for safeguarding reasons
- Emergency services
- Organisations we're legally obliged to share personal information with

Compliance and Enforcement

1. Duty of Confidentiality

We are subject to the **Common Law Duty of Confidentiality**. The Common Law Duty of Confidentiality is a legal obligation requiring that information shared in confidence must not be disclosed without the consent of the person who provided it.

However, there are circumstances where we will share relevant health and care information. These are where:

- you've provided us with your consent (we have taken it as implied to provide you with care, or you have given it explicitly for other uses);
- we have a legal requirement (including court orders) to collect, share or use the data;
- on a case-by-case basis, the public interest to collect, share and use the data overrides the public interest served by protecting the duty of confidentiality (for

example sharing information with the police to support the detection or prevention of serious crime);

- If in England or Wales – the requirements of The Health Service (Control of Patient Information) Regulations 2002 are satisfied; or
- If in Scotland – we have the authority to share provided by the Chief Medical Officer for Scotland, the Chief Executive of NHS Scotland, the Public Benefit and Privacy Panel for Health and Social Care or other similar governance and scrutiny process.

2. Contracts, Data Sharing Agreements and Service Level Agreements

The Company will ensure that any commercial arrangements with organisations to provide additional services that require the sharing of personal data are covered either

- a) in the initial contract/agreement with the organisation for the services that they will provide and how they will process the data.

Or

- b) With a specific data sharing agreement and/or Service Level Agreement between the Company and the Organisation providing the additional services. Any such documentation should cover what information is required, why and how this will be used by the Organisation if this is not covered as part of any initial contract/agreement.

The Company expects to be informed, at the earliest, most practicable opportunity, of any data breaches within the partner organisation. The Company will monitor, in compliance with a) or b), the relationship and service delivered.

The Company reserves the right to review any ongoing agreements with organisations using data provided by the company, particularly in relation (but not limited to) data breaches within the partner organisation.

3. Complaints

If you have any concerns about the Company use of personal data, you can make a complaint to us using the contact details at the top of this privacy notice.

If you remain unhappy with how we've used your data after raising a complaint with us, you can also complain to the ICO.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

Website: <https://www.ico.org.uk/make-a-complaint>

Related Policies

Complaints Policy

Equality, Diversity and Inclusion Policy

Recruitment and Selection Policy