

Patient and Third Party Privacy Notice

1 Overview

1.1 Cumbria Health whose registered office is 4 Wavell Drive, Rosehill Industrial Estate, Carlisle, CA1 2SE is a **Data Controller**. This means that we determine the purpose and means of the processing of your Personal Data.

1.2 Cumbria Health is required to appoint a Data Protection Officer (DPO) in respect of our processing activities. Cumbria Health uses an external DPO whose details are set out below:

Yvonne Salkeld
Head of Information Governance
North Cumbria Integrated Care
Maglona House, Unit 68, Kingstown Broadway, Carlisle, CA3 0HA
Tel: 01228 603927

You should contact the DPO if you have any concerns about the information contained in this privacy notice or data protection within Cumbria Health generally.

1.3 Cumbria Health takes the security and privacy of your data seriously. We need to gather and use information about you as part of our business, to provide the best care to patients, ensure patient safety and to manage our relationship with patients and third parties. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a legal obligation to provide the information contained in this policy.

1.4 This policy applies to all patients, service users and third parties (excluding job applicants) whose personal data we process as a result of our business

activities and service provision. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy.

1.5 Cumbria Health has a separate privacy notice in respect of job applicants, which can be viewed via the following link <https://www.chocltd.co.uk/recruitment/>.

1.6 Cumbria Health has measures in place to protect the security of your data in accordance with our Data Protection, Information Governance, Records Management, Information Security, and Email and Internet Use policies.

1.7 Cumbria Health will hold data in accordance with our Records Management Policy. We will only hold data for as long as necessary for the purposes for which we collected it.

1.8 This notice explains how Cumbria Health will hold and process your information.

1.9 It is intended that this privacy notice is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this notice, Cumbria Health intends to comply with the 2018 Act and the GDPR.

2 Data Protection Principles

2.1 Personal data must be processed in accordance with six 'Data Protection Principles.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and

- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

3 How we define personal data

3.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

3.2 This policy applies to all personal data relating to data subjects whether it is stored electronically, on paper or on other materials.

3.3 This personal data might be provided to us by you, someone else (such as a relative, the NHS 111 service, your doctor or an independent doctor acting on our behalf), a practice owned and/or operated by us or it could be created by us.

3.4 We will collect and use the following types of personal data about you:

- Name and address and contact telephone number;
- date of birth;
- the contact details for your emergency contacts;
- your gender;
- your marital status and family details;
- your health records and genetic data;
- your identification documents including passport and driving licence;
- your images (whether captured on CCTV, by photograph or video); and

- any other category of personal data which we may notify you of from time to time.

4 How we define special categories of personal data

4.1 **'Special categories of personal data'** are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your religious or philosophical beliefs;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

5 How we define processing

5.1 **'Processing'** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;

- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

6 How will we process your personal data?

6.1 Cumbria Health will process your personal data (including special categories of personal data) in accordance with our obligations under GDPR and the 2018 Act.

6.2 We will use your personal data for:

- performance of tasks carried out in the public interest or in the exercise of official authority vested in us as a controller (in respect of the provision of health services to patients and service users);
- where it is necessary to protect your vital interests;
- complying with any legal obligation;
- Where we need to perform the contract we are about to enter into or have entered into with you; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 10 below. This bullet point is not relevant for patients and service users and will only be relied upon in respect of other third parties such as suppliers.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not be able to provide our services to you.

7 Examples of when we might process your personal data

7.1 We have to process your personal data in providing primary care health services as follows and in each case the lawful basis will be the performance of official authority vested in us or, in life-threatening situations involving you, to protect your vital interests:

- Decisions made by health professionals or support staff when treating you or assessing the best course of treatment for you;
- Liaising with other NHS Organisations, other practices owned and/or operated by us and health professionals in relation to your care and health records;
- Improving our service provision for future service users;
- Preparing statistics on NHS performance and activity;
- Administration;
- Investigating concerns and complaints;
- Obtaining payment for services provided;
- Training and education of staff, including assessing performance. to decide how much to pay you, and the other terms of your contract with us;
- Research and analysis; and
- For any other reason which we may notify you of from time to time.

7.2 For third parties who are not patients or service users, we will process your personal data as follows:

- To manage payments, fees and charges and collect money owed to us;
- To manage our relationship with you, including providing you with relevant information;

- To enable you to perform the contract you have entered into with us and vice versa.

7.3 We will process special categories of your personal data (see above) in certain situations in accordance with the law. For example, in the provision of primary care health services we are permitted by the 2018 Act and GDPR to process your data where:

- it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- it is necessary for the purposes of preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services; or
- it is necessary for the reasons of public interest in the area of public health.

7.4 If we require your explicit consent for processing (which will be rare) then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the DPO.

7.5 We will not process special category data for any third party who is not a patient or service user, other than for recruitment, which is covered by a separate privacy notice as detailed above.

7.6 We do not make automated decisions about you using your personal data or use profiling in relation to you.

8 Sharing your personal data

8.1 We will share your personal data, including health data with other health and adult social care organisations as necessary, in addition to the various practices owned and operated by us as necessary. We are required to do this by law in order to improve the care provided to you.

8.2 Sometimes we might share your personal data with our contractors and agents, including Doctors who are not employees of Cumbria Health, in order to carry out our obligations under our contract to provide primary care health services.

8.3 Personal data shared with other health and adult social care organisations is subject to legal safeguards imposed on the recipients. Where we share personal data with anyone who is not subject to such legal safeguards, we require those organisations or individuals to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

8.4 We do not typically transfer personal data outside the UK. We will only transfer your personal data out of the UK in the following circumstances:

- It is to countries that have been deemed to provide an adequate level of protection for personal data by the Secretary of State;
- Where we can ensure that appropriate safeguards are in place with the recipient in accordance with the Data Protection Act 2018; or
- The transfer is otherwise permitted pursuant to the Data Protection Act 2018

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the UK.

8.5 GP Practices managed by Cumbria Health use a processor, iGPR Technologies Limited (“iGPR”), to assist us with responding to report requests relating to your patient data, such as subject access requests that you submit to us (or that someone acting on your behalf submits to us) and report requests that insurers submit to us under the Access to Medical Records Act 1988 in relation to a life insurance policy that you hold or that you are applying for. iGPR manages the reporting process for us by reviewing and responding to requests in accordance with our instructions and all applicable laws, including UK data protection laws. The instructions we issue to iGPR include general instructions on responding to requests and specific instructions on issues that will require further consultation with the GP responsible for your care.

9 Subject access requests

9.1 Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them.

9.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to Cumbria Health. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

9.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

10 Your data subject rights

10.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

10.2 You have the right to access your own personal data by way of a subject access request (see above).

10.3 You can correct any inaccuracies in your personal data. To do so you should speak to a member of our staff or contact our DPO.

10.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should speak to a member of our staff or contact our DPO.

10.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact our DPO.

10.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

- 10.7 You have the right to object if we process your personal data for the purposes of direct marketing.
- 10.8 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller in limited circumstances. We will not charge for this and will in most cases aim to do this within one month.
- 10.9 With some exceptions, you have the right not to be subjected to automated decision-making.
- 10.10 You have the right to be notified of a data security breach concerning your personal data.
- 10.11 In most situations we will not rely on your consent as a lawful ground to process your data. If we do request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact our DPO.
- 10.12 You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

11 Data Security

- 11.1 We have put in place measures to protect the security of your data. We will keep our working practices under review and update them as necessary to protect personal data.
- 11.2 Third parties will only process your data on our instructions and where they have agreed to treat the data confidentially and to keep it secure.
- 11.3 We have put in place appropriate security measures to prevent your data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your data to those employees, agents,

contractors and other third parties who have a business need to know. They will only process your data on our instructions and they are subject to a duty of confidentiality.

11.4 We have procedures in place to deal with any suspected data security breach and will notify you and the Information Commissioner's Office of a suspected breach where we are legally required to do so.

12 Data retention

12.1 We will only retain your data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal data are available in our Records Management Policy. Please contact our DPO if you would like to see a copy of our Records Management Policy. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

12.2 In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.