

Document Title	ELMS Privacy Notice
Date	27 th April 2021
Review date	1 March 2023
Version Number	2
Supersedes	version 1
Notes	Update of contents Uploaded to GPTN.

Current versions of documents are held in GP Team Net. Printed copies are uncontrolled

ELMS Declaration:**To support the care we give you we will be making use of some of your data**

This privacy notice sets out the way East Lancashire Medical Services process your personal information - how we collect information, what we do with it, how we protect it and what controls or rights you have.

We are committed to protecting the privacy of our patients and anyone who interacts with us and will treat all information you give us with care.

We promise to:

- Tell you why we collect personal information, how we do this and what we use it for.
- Only collect the information we need to deliver the service to you.
- Keep the personal information up to date and ensure it is safe and secure.

Please read this Privacy Policy carefully to understand how we process your personal data. By providing your personal data to us or by using our services or this website you are accepting or consenting to the practices in this Privacy Policy.

We may change this policy from time to time and the date this policy was last updated is shown at the end of this document.

1. Overview

- 1.1 East Lancashire Medical Services Limited (“ELMS”) whose registered office is St Ives House, Accrington Road, Blackburn BB1 2EG is a not for profit social enterprise registered with the Financial Conduct Authority as a society under the Co-operative and Community Benefit Societies Act 2014 – registration number IP30263R.
- 1.2 ELMS are a Data Controller - this means that we determine the purpose and means of the processing of your Personal Data – and we are recorded on the ICO Data Protection Register under registration number Z114667.
- 1.3 ELMS is required to appoint a Data Protection Officer (DPO) in respect of our processing activities and has an internal DPO who can be contacted via info.elms@nhs.net You should contact the DPO if you have any concerns about the information contained in this privacy notice or data protection within ELMS generally.
- 1.4 ELMS 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. ELMS intend to comply with its 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.
- 1.5 This policy applies to all patients, service users and third parties (including job applicants) whose personal data ELMS 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 ELMS 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.
- 1.6 ELMS 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 ELMS collected it.
- 1.7 This notice explains how ELMS will hold and process your information.
- 1.8 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, ELMS intends to comply with the 2018 Act and the GDPR.

2. Data Protection Principles

- 2.1 ELMS looks to process personal data in accordance with six 'Data Protection Principles' that say 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.

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

3. 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), or it could be created by us.

3.4 ELMS 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 ELMS may notify you of from time to time.

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

5. 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 ELMS Process Personal Data?

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

6.2 ELMS 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 direct health services to patients and service users);
- where it is necessary to protect your vital interests;
- complying with any legal obligation;
- Where ELMS needs to perform the contract we are about to enter into for the delivery of patient care or have entered into with you; or
- If it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, ELMS 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 ELMS 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.

ELMS 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 ELMS 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 ELMS might process your personal data

7.1 ELMS has 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 lifethreatening 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 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, ELMS 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 ELMS 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 ELMS 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 ELMS requires your explicit consent for processing (which will be rare) if there is no other legal ground to process 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 ELMS 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 ELMS does not take automated decisions about you using your personal data or use profiling in relation to you.

8. Sharing Personal Data

8.1 Your information will only be accessible to our staff and clinical performers only where it is appropriate in respect of the role they are carrying out. Sometimes ELMS might share your personal data with our contractors and agents, including Doctors who are not employees of ELMS, in order to carry out our obligations under our contract to provide primary care health services.

- 8.2 ELMS will share your personal data, including health data with other health and social care organisations as necessary. We are required to do this by law in order to improve the care provided to you and any personal data shared is subject to legal safeguards imposed on the recipients.
- 8.3 The organisations, health and social care professionals and others we might share your data with might include:
- Doctors, clinicians, hospitals, clinics, diagnostic and treatment centres and other health care providers to provide our services and continuity of health care;
 - Your host GP – You can ask us not to do so and we will respect this unless legally required to provide the information but it may be detrimental to your health if your GP does not have your full medical history.
 - First responders, ambulance service, safeguarding professionals within the NHS and Local Authorities, undertakers, the local coroner and care homes.
 - Organisations or people who by law or regulations we must share your personal information with e.g. national data bases, screening registers government authorities and NHS organisations.
 - The police or other law enforcement agencies to assist them perform their duties if we must do this by law or under a court order.
 - Where we use other organisations to provide services on our behalf for processing, mailing, delivering, sending mail and emails, data analysis, assessment and profiling or processing payments.
 - Providers of IT systems, support and hosting in relation to IT systems on which information is stored. Where a third-party data processor is used, we ensure they operate under a contract which includes confidentiality and security of personal data and their obligations under the Data Protection legislation.
 - To organisations who you have requested us to supply information so that they can provide services or products you have requested. • When using auditors and professional advisors.
 - When we are legally required to, or because of a lawful request by a governmental or law enforcement authority.
 - If we merge with another organisation or form a new entity.
- 8.4 Where ELMS 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 ELMS 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.

8.5 The systems we use are web based which means that data is transferred over the secure NHS N3/HSCN network to the data centre. None of this data will be transferred outside the EU. If this changes you will be notified, we will only undertake such transfers where ELMS can ensure adequate safeguards are in place and we will explain those safeguards to you.

9. Subject Access Requests

- 9.1 Data subjects can make a 'subject access request' ('SAR') to find out the information ELMS 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 our Company Secretary at our office address: St Ives House, Blackburn Road, Blackburn BB1 2EG. 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 ELMS 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). For patients wishing to view their medical record, the best way to do this would be through your own GP as ELMS do not hold the master copy.
- 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 ELMS 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 in the first instance 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 ELMS 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. ELMS do not undertake 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. ELMS 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 ELMS 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 on 0303 123 1113 or at their website www.ico.org.uk This website has further information on your rights and our obligations.

11. ELMS National Data Opt-Out Policy statement

11.1 Introduction

The national data opt-out applies to the disclosure of confidential patient information for purposes beyond individual care across the health and adult social care system in England. ELMS does not disclose or share information beyond that which is required for direct patient care and in line with the National opt exemptions identified below

Notwithstanding this, this document provides operational guidance to understand the application of national data opt-out policy – it sets out when the national data opt-out must be applied along with the exemptions when it will not apply. The national data opt-out applies to data that originates within the health and adult social care system in England and is applied by health and care organisations that subsequently process this data for purposes beyond individual care. The opt-out does not apply to data disclosed by providers of health and care services outside of England or to children's social care services.

11.2 Health and adult social care system

The national data opt-out applies to data that originates within the health and adult social care system in England. The following organisations are considered to be part of the health and adult social care system in England and must consider whether they are required to apply the national data opt-out:

- Department of Health and Social Care and other national bodies e.g. NHS England
- NHS and Local Authorities providing health and adult social care services in England;

And

- other organisations or persons who provide health or adult social care services in England under arrangements agreed with any organisation covered in the above 2 bullet points.

This definition is aligned to the Health and Social Care Act 2012 Section 250, which defines the organisations required to have regard to published information standards. Such organisations need to assess whether any of their data disclosures require the opt-out to be applied – some organisations may not have any data uses that are in scope.

11.3 Specific Inclusions

For the avoidance of doubt confidential patient information generated or processed by private providers, including Any Qualified Providers (AQPs) such as ELMS who provide health and adult social care services which are funded or under contract with a public body, such as a Clinical Commissioning Group must consider national data opt-outs when processing data for purposes beyond individual care in line with the wider policy:

11.4 When does a national data opt-out not apply?

The following are exemptions from the national data opt-out:

- Consent

The national data opt-out does not apply where explicit consent has been obtained from the patient for the specific purpose.

The application of the national data opt-out when researchers are seeking to contact a cohort of patients to ask their consent (so called consent for consent)

- Communicable diseases and risks to public health

The national data opt-out does not apply to the disclosure of confidential patient information required for the monitoring and control of communicable disease and other risks to public health.

This includes any data disclosed where Regulation 3 of The Health Service (Control of Patient Information) Regulations 2002 provides the lawful basis for the common law duty of confidentiality to be lifted. Public Health England oversees the use of this legal gateway on behalf of the Secretary of State for Health and Social Care. Regulation 3 allows confidential patient information to be lawfully processed with a view to:

- diagnosing communicable diseases and other risks to public health
- recognising trends in such diseases and risks
- controlling and preventing the spread of such diseases and risks
- monitoring and managing:
 - outbreaks of communicable disease
 - incidents of exposure to communicable disease

- the delivery, efficacy and safety of immunisation programmes
 - adverse reactions to vaccines and medicines
 - risks of infection acquired from food or the environment (including water supplies)
 - the giving of information to persons about the diagnosis of communicable disease and risks of acquiring such disease.
- Overriding public interest

The national data opt-out does not apply to the disclosure of confidential patient information where there is an overriding public interest in the disclosure, i.e. the public interest in disclosing the data overrides the public interest in maintaining confidentiality.

This should be because of a positive public interest test having regard to the circumstances of the case. Data controllers are expected to have their own arrangements in place to apply the public interest test as and when necessary.

- Information required by law or court order

The national data opt-out does not apply to the disclosure of confidential patient information where the information is required by law or a court order.

- Payments and invoice validation

The following policy statements apply to data processing in support of payments and invoice validation:

- Unless there is no alternative, data flows for payments and invoice validation should not use identifiable data. In such cases anonymised data can almost certainly be used and national data opt-outs would not apply - provided data is anonymised in line with the ICO Code of Practice on anonymization.
- National data opt-outs do not apply where a patient has given their explicit consent for the use of their data for payment and invoice validation. All organisations within health and adult social care should be as transparent as possible as to how confidential patient information is being disclosed for payment purposes in order to better manage patient expectations.
- In accordance with the recommendations made in the NDG review, national data opt outs do not apply to data disclosed for the purpose of non-contracted invoice validation (non-contracted activity refers to services delivered by a health or care provider, where there is no agreed contract with the patient's responsible commissioner e.g. a patient receiving treatment in area that is outside of the CCG area where they are registered).

- National data opt-outs do not apply to data disclosed to NHS BSA for the payment of prescription charges, specifically where the data is disclosed under Regulation 18A of the National Health Service (Pharmaceutical Services, Charges and Prescribing) (Amendment) Regulations 201811.

11.5 Compliance with the national data opt-out

The national data opt-out is a policy set by the DHSC and gives effect to the right set out in the NHS Constitution to “request that your confidential information is not used beyond your own care and treatment”. The policy is intended to implement the recommendations of the NDG review and thereby help to increase public confidence and trust in the use of their health and care data.

A number of mechanisms have been put in place to ensure that organisations within health and adult social care comply with the national data opt-out policy as required. Principally this is a combination of information standards, statutory guidance, contractual levers, legal requirements and information for the public to increase visibility and transparency of compliance at a local level.

It should be noted that health and adult social care bodies are legally required to “have regard to” information standards²⁰ and statutory guidance²¹. Whilst these are not an absolute legal obligation - an organisation that does not comply with an information standard or statutory guidance may be leaving themselves open to legal challenge.

The declaration below demonstrates how ELMS would seek to offer you exemption, should this be required:

Your confidential patient information can be used for improving health, care and services, including:

- planning to improve health and care services
- research to find a cure for serious illnesses

Your decision will not affect your individual care and you can change your mind anytime you like.

I allow/do not allow my confidential patient information to be used for research and planning.

12. Data Security

12.1 The security of your personal information is very important to us. ELMS has put appropriate organisational and technical measures in place to prevent unauthorised access or unlawful processing of personal data and to prevent data being lost, destroyed or damaged. We will keep these arrangements under review and update them as necessary to protect personal data.

12.2 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.

12.3 ELMS has 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.

12.4 ELMS has 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.

13. Data Retention

13.1 ELMS 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.

13.2 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.

For example, our premises in Blackburn are monitored by CCTV for purposes of crime prevention and for the safety of visitors and staff; images are retained for 30 days in accordance with ICO guidelines. They are stored for approximately 30 days before being overwritten and we will not share these images with anyone outside ELMS other than the police, should the need arise.

13.3 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 this Policy.

13.4 In some circumstances ELMS 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.

14. Cookies

14.1 Cookies are used on most websites including this one to collect information and improve user access. A cookie is. When you visit a website that uses cookies, the website sends a cookie - a small text file that contains a unique label or ID number - to your browser's software and is stored on your computer after you leave the site; when you return to the website at a later date the website recognises you using the cookie.

14.2 ELMS do not use these cookies for its own marketing or commercial benefit that are operated by the website platform provider – My Surgery Website – whose statement in respect of privacy and usage is detailed at <https://www.mysurgerywebsite.co.uk/disclaimer.htm>

- 14.3 Most web browsers automatically accept cookies but, if you prefer, you can change your browser to prevent that or to notify you each time a cookie is set; www.allaboutcookies.org will provide information on settings within your browser as well as other useful information on cookies.
- 14.4 Please note however, that by blocking or deleting cookies you may not have full use of the website. If you continue using this site we will assume that you are happy to receive all cookies and reserve the right to amend, remove or add new cookies and similar technical tools at any time.

15. Links to Other Websites

- 15.1 ELMS website contains links to other websites and partners. ELMS do not control over those websites and we cannot be responsible for the protection and privacy of any information which you provide whilst visiting other websites and such sites are not governed by this privacy statement.

16. Contacting us

- 16.1 If you have any questions you can email them to us at info.elms@nhs.net. Through this email address you can contact the Data Protection Officer (who is in control of data protection issues at ELMS) and we can advise you on where to make complaints about data protection issues.

East Lancashire Medical Services Limited
St Ives House
Accrington Road
Blackburn BB1 2EG

info.elms@nhs.net