The London Ambulance Service NHS Trust privacy notice for the purposes of individual care, the provision of best care, employment and staffing.

This privacy notice tells you what to expect us to do with your personal information when you contact us or use our services.

You can find more detailed information about how we use your information for the following specific purposes here:

- Research - https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/templates/template-wording-for-generic-information-document/ how health researchers use information
- Research within the LAS – **https://www.londonambulance.nhs.uk/about-us/research/#**
- Cookies – https://www.londonambulance.nhs.uk/privacy-policy/

Our contact details

Name: London Ambulance Service NHS Trust

Address: Headquarters: Waterloo

220 Waterloo Road
London
SE1 8SD

Our telephone number is 020 7783 2000.

- General Information Governance/Data Protection inquiries email address: londamb.ig@nhs.net

- Website: https://www.londonambulance.nhs.uk/

- We are the controller for your information. A controller decides on why and how information is used and shared.

Data Protection Officer contact details

- Our Data Protection Officer is Philip John, who is also our Information Governance Manager, and is responsible for monitoring our compliance with data protection requirements. You can contact him with queries or concerns relating to the use of your personal data at philip.john1@nhs.net

How do we get information and why do we have it?

The personal information we collect is provided directly from you for the provision of patient care, research, staff training, general enquiries, and any additional correspondence we may receive from you.

We log details electronically when we receive a call for help at our emergency control centres or 111 service, or book a non-emergency transport service that we operate.

If one of our ambulances attends you, or you are transferred between hospitals by ambulance, we will collect information about you to help us identify and treat you. This will be written on a patient clinical record along with details of your symptoms, condition, and any treatment we give you. We are also required to record details of your ethnicity and other information to help us monitor the equality of the services we provide.

If you speak to one of our 111 call handlers or clinical advisors we will record your details and access your clinical information in order to provide the advice or care you need, which may include transferring you to the out-of-hours service, requesting an ambulance or, if it is in hours, putting you in touch with your dentist or GP. Patients may be put at risk if those who provide their care do not have access to relevant, accurate and up-to-date information about them.

If you receive non-emergency transport services, we will record details about where you live, where we will be taking you and some details about your circumstances.

If you make a complaint or an enquiry about the service we have provided, or have contact with us on another matter, we will keep a record of all the relevant details in a file for case management purposes. In some cases, we may need to obtain information from the hospital we took you to in order to investigate a complaint or deal with an enquiry.

In conjunction with London's Air Ambulance we also use a facility to obtain a secure live-stream video from callers' mobile phones at certain incidents, to help our control room clinicians more accurately and rapidly assess patient injuries. This will only be done when clinically necessary with patient and caller consent, or when a patient is unable to consent it will be done in a patient's best interests. Footage will only be stored when necessary in line with existing Trust policies and destroyed when no longer required.

The London Ambulance Service utilises surveillance cameras (Static/Vehicle based CCTV and Body Worn Cameras) in and around the Trust's sites, on our emergency vehicles, as well as body worn cameras used by operational crews which has been rolled out nationally following a successful local pilot.

Please note: Our surveillance cameras inside our vehicles and our body worn cameras are only activated by the crew when they feel there may be a risk to safety. Should these systems be activated, the crew will advise you and/or an audio message will be played inside the vehicle with a recording flashing light on the body worn cameras.

We also receive personal information about you indirectly from others, in the following scenarios:

- from other health and care organisations involved in your care so that we can provide you with care; and
- from family members or carers to support your care

What information do we collect?

Personal information

We currently collect and use the following personal information:

Names; dates of birth; NHS numbers; addresses, email addresses, telephone numbers, fax numbers and IP addresses when you contact us over the website.

More sensitive information

We process the following more sensitive data (including special category data):

- data concerning physical or mental health (for example, details about your appointments or diagnosis);
- data revealing racial or ethnic origin;
- data concerning a person's sex life;
- data concerning a person's sexual orientation;
- genetic data (for example, details about a DNA sample taken from you as part of a genetic clinical service);
- biometric data (where used for identification purposes; and
- data revealing religious or philosophical beliefs.

Who do we share information with?

We may share information with the following types of organisations:

If an ambulance takes you to hospital, we will share an electronic copy of the patient clinical record so that they have details of your condition and the treatment we have provided.

In addition to sharing your data with other clinicians, we can access your data from other health and care organisations across London to ensure we are providing you with the best possible care.

Where necessary, we use a limited number of private contractors to supplement our emergency and non-emergency transport services. In these cases, they are under contract to us and must comply with data protection legislation in the same way we do. Their performance is monitored and all the information they collect about you is transferred securely to us.

Other health and social care professionals involved in your treatment or care may ask us for information about your use of our services or the treatment you received. Provided we are satisfied that they need this information for your care, or you have given your permission, we will provide this to them.

In some circumstances we may share information or clinical records with other healthcare professionals – most commonly your GP but also specialist healthcare teams such as social service – even if we have not taken you to hospital or provided 111 advice. We do this to help them assess whether they can offer you support that may help to prevent a similar situation arising again.

We are sometimes also asked by the Clinical Commissioning Groups (CCGs) that fund our services to provide information about incidents attended so they can identify and provide more appropriate care pathways for patients. The information we provide will not identify you.

Where another NHS organisation is funding a non-emergency transport service journey, we have to confirm personal information – although we will only provide the minimum of information required.

We will not disclose your information to third parties outside the NHS without your permission unless it is required for your direct care or there are exceptional circumstances. This can include, where it is necessary for the performance of the task carried out in the public interest or the public good outweighs your right to confidentiality, for example:

- when a serious crime has been committed;
- if there are risks to the public or NHS staff;
- to protect vulnerable children or adults who are not able to decide for themselves whether their information should be shared;

- we need to use the information for medical research. We have to ask permission from the Confidentiality Advisory Group (appointed by the NHS Health Research Authority)
- Trust performance auditing and accreditation by Third party providers:

or we have a legal duty to do so, for example:

- when a court order has been issued;
- where a public inquiry requires the information;
- reporting some infectious diseases, or wounding by firearms.

We will seek your consent before we release information that identifies you to any third party for any other reason than direct patient care and those set out above.

Your information is never collected for direct marketing purposes, and is not sold on to any other third parties. Any data processed in a third country will only be approved following the completion of a Data Protection Impact Assessment, a Digital Impact Assessment, a Third Party Supplier Questionnaire and will also be subject to UK GDPR regulations regarding the processing of data in a third country.

Please note, anonymised or redacted information shall be shared to third parties such as, but not limited to, research bodies and media outlets. To ensure anonymity and possibilities of re-identification, the London Ambulance Service NHS Trust undertakes relevant appropriate privacy and security assessments before any disclosure.

The London Ambulance Service routinely reviews the outcomes of its patients in order to improve the quality and efficiency of its care. As part of this, the Service shares routine feedback with its staff on their patients' outcomes, providing clinical staff with reflection and learning opportunities, and supporting them to continuously improve their care. To enable this, Acute hospital NHS Trusts in London share information about the hospital treatment and outcomes of patients first treated by the London Ambulance Service.

In addition, the London ambulance Service may also analyse the data from London hospitals, to provide visibility on improvements which may need to be made to the emergency pathways of patients using London Ambulance Services. This analysis is made available to London Ambulance Staff Members and Acute London NHS Trusts, in an aggregated manner that will not identify you.

The sharing of patient data included in the My Clinical Feedback project is for Direct Care purposes which allows implied consent to be relied upon under the common law duty of confidentiality. The legal basis for the processing of this data under UK General Data Protection Regulation (UK GDPR) are:

- 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.

- Article 9 (2) (h): Processing is necessary for medical diagnosis, the provision of health care, or the treatment or management of health care services and system (Health Care) plus Schedule 1, Part 1, Paragraph 2 'Health or social care purposes' of DPA 2018.

NHS111PS – NHS 111 Patient Experience Surveys

As a provider of NHS 111 / IUC Services LAS will periodically survey their 111 callers to gather feedback, and supply that anonymised data to NHS England every six months.

The data gathered includes your satisfaction with NHS 111, whether advice was followed, if the problem improved, and what you would have done if NHS 111 was not available.

NHS 111 - Patient Demographic Web Forms

Content: The 111 Caller Demographics project introduces a Visual Interactive Voice Response (IVR) capability within the NHS 111 service, enabling callers to voluntarily enter their demographic details via a secure webform while waiting in the telephone

queue. Where eligible, callers receive an SMS containing a link to the web form, which collects core demographic information (e.g. name, date of birth, address) required for NHS 111 case creation. This information is linked to the caller's phone number and automatically presented to the call handler within Adastra when the call is answered.

The project is designed to improve operational efficiency and patient flow within the NHS 111 service by reducing the time call handlers spend collecting demographic information during live calls and relies upon the consent of the caller to engage this functionality.

Using call recordings for safety campaigns

To help protect our colleagues and the public, London Ambulance Service may occasionally use short extracts from calls in safety and awareness campaigns. These campaigns aim to explain the impact of abusive or inappropriate behaviour and encourage people to treat our colleagues with respect.
Any extract used publicly will be anonymised. We will remove names, contact details, locations, clinical information and other details that could identify the caller, patient or anyone else involved. Voices will also be altered where necessary and only the minimum amount of audio needed will be used. Identifiable recordings will not be published.

Automation, Ambient Voice Technology and Artificial Intelligence

The London Ambulance Service is committed to providing high-quality care while ensuring the privacy and confidentiality of your personal information. As part of our ongoing efforts to enhance patient care, we are assessing and adopting a number of advanced technology solutions, including Automation Technology, Ambient Voice Technology and Artificial Intelligence tools to support the service we provide.

These Tools include, but are not limited to:

- **TORTUS** - A medical AI ambient voice application designed to streamline clinical documentation by both transcribing patient conversations in real-time and allowing clinician dictation, to support drafting of medical notes, letters, and coding suggestions. As with any digital products involving patient information, this product is subject to strict governance arrangements including MHRA regulation. Clinicians always check and validate records created with the support of AI.
- **Copilot** – Microsoft's Enterprise 365 Copilot is a generative AI product. It automatically inherits the existing security, compliance, and privacy policies

for Microsoft 365. Microsoft 365 Copilot processes data without storing it. User data is not used to 'retrain' the Copilot large language model. Results are returned from Copilot to the user, and are provided for the user to choose to use or disregard. Copilot only processes patient data to conduct thematic reviews of trends via patient surveys and is outputted in aggregated, non-identifiable outputs only. It may only be used to process staff data in approved situations. In all use cases LAS will ensure correct governance is in place.

- **Blue Prism** – Automated task processing application that is currently deployed to support staff in accessing organisational and policy information within the organisation.

How we use or plan to use Automation, Ambient Voice Technology and Artificial Intelligence tools:

- Enhanced Care: Automation, Ambient Voice Technology and Artificial Intelligence technology to assist our healthcare professionals in delivering efficient and effective care. This includes supporting clinical decision-making and improving the efficiency and content of medical records.
- Data Processing: The Automation, Ambient Voice Technology and Artificial Intelligence tools may process personal, special category, and confidential data. This processing is conducted in line with the reasonable expectations of our patients and complies with data protection laws.
- Privacy and Security: We ensure that all data processed by Automation, Ambient Voice Technology and Artificial Intelligence tools are handled securely and confidentially. Our systems are designed to protect your information and uphold your rights under the UK Data Protection Act 2018 and GDPR. In cases where an Automation, Ambient Voice Technology and Artificial Intelligence tools are implemented within the Trust they will only be approved following the completion of a Data Protection Impact Assessment.
- Transparency: We are committed to transparency about how your data is used. If you have any questions or concerns about the use of AI technology in your care, please do not hesitate to contact us.

Automated Decision-Making

We may use your information to support automated decision-making alongside human involvement. These automated systems may have a significant potential impact. Examples include systems to communicate concerns around safeguarding and those involved in ensuring the earliest possible dispatch of ambulances for the highest priority emergencies. In cases where automated decision-making is implemented within the Trust, it will only be approved following the completion of a Data Protection Impact Assessment, and will also be subject to UK GDPR regulations regarding the rights of individuals relating to automated decision-making.

Lawful Basis for how we use Automation, Ambient Voice Technology and Artificial Intelligence tools

The lawful basis to process your personal data does not change because we use Automation, Ambient Voice Technology and Artificial Intelligence tools and can be viewed under the 'What is our Lawful Basis for using information' section of this Privacy Notice.

Helping us to train our staff and monitor their work

Clinicians may need a copy of the patient clinical records they have completed for their training, but they will blank out information which could identify you before they do this. London Ambulance Service Paramedics may receive clinical feedback on the outcomes and associated treatments of the patients they have attended, to support their learning and development to improve the care they provide.

All requests for third party listening will be considered in line with the Caldicott Principles and must be approved in advance by the Director of 999 Operations. Examples of third parties include approved appropriate representatives from external health and social care organisations, regulators or representatives from other ambulance services. Approval to listen to calls will be maintained in a log which will be shared with the Senior Clinical Lead - 999 Operations for auditing purposes. Any requests outside of the aforementioned groups should be approved by the Senior Clinical Lead - 999 Operations who may seek advice from the Caldicott Guardian.

Monitoring the standard of care we provide and undertaking research

Anonymised information from patient clinical records is also used for internal audit purposes and details of the emergency treatment and care we provide is sometimes used for research. We make sure ethical approval has been obtained in accordance with NHS guidelines before we release any information outside the organisation for research purposes and do not release information that could identify patients unless there is a legal basis for doing so.

On occasion we may need to view records that contain personal information and use this information to link records to allow us to get a full picture of the care provided to you. If you do not wish for us to use your data for research in this way please contact the Clinical Audit & Research Unit at londamb.CARU.Enquiries@nhs.net

Monitoring the standard of care provided within the NHS overall

We pass information to other NHS organisations as part of national initiatives to monitor the standard of care provided within the NHS as a whole. In all cases, we supply only the details that are needed for these purposes and, wherever possible, the information will be anonymised.

Information relating to your health and wellbeing and other special category data

We use the following information to comply with our legal obligations and for equal opportunities monitoring. We also use it to ensure the health, safety and wellbeing of our employees.

- Health and wellbeing information either declared by you or obtained from health checks, eye examinations, occupational health referrals and reports, sick leave forms, health management questionnaires or fit notes i.e. Statement of Fitness for Work from your GP or hospital.
- Accident records if you have an accident at work.
- Information provided with consent to match appropriate alternative duties hub placements.
- Details of any desk audits, access needs or reasonable adjustments.
- Information you have provided regarding Protected Characteristics as defined by the Equality Act and s.75 of the Northern Ireland Act for the purpose of equal opportunities monitoring. This includes racial or ethnic origin, religious beliefs, disability status, gender identification and may be extended to include other protected characteristics.

What is our lawful basis for using information?

Personal information

Under the UK General Data Protection Regulation (UK GDPR), the lawful basis we rely on for using personal information is:

- the NHS is an official authority with a public duty to care for its patients, as guided by the Department of Health
- Data protection legislation states that it is appropriate to do so for the health and social care treatment of patients, and the management of health or social care systems and services.

If we need to use your personal information for any reason beyond those stated above and below, we will discuss this with you. You have the right to ask us not to use your information for certain purposes but there are exceptions to this which are listed under ‘Who do we share information with’.

Under UK GDPR the professionals involved in your individual care (or direct care) will be using implied consent from you to see your shared medical records. In order for the sharing of Personal Data to comply with Article 5 of the General Data Protection Regulation it must be fair and lawful and one of the Article 6 conditions must be met. Article 9 conditions must also be met if Sensitive Personal Data or special category data is being shared. The following articles are the ones that apply for sharing of data for the professionals involved in your care:

- A) Article 6 condition – The sharing of Personal Data is permitted under Article 6 paragraph (a) consent freely given; paragraph (c) (processing for legal obligation); paragraph (e) (public interest or in the exercise of official authority); and/or paragraph (f) (processing for the purpose of legitimate interests).
- B) Article 9 condition – The sharing of Sensitive Personal Data or Special Category Data is permitted under Article 9 (h) (processing for medical purposes); paragraph (i) (public interest in the area of public health) and/or paragraph (j) Archiving, research and statistics. For the vast majority of sharing we will be relying on article (h) with an implied consent model for direct individual care (more detail below where we talk about the Common Law Duty of Confidentiality). In certain instances, however, we may also rely on paragraph (a) (explicit consent) or paragraph (c) (vital interests) but these will be specified in any sharing agreements or data processing contracts related to those special cases.

Common Law Duty of Confidentiality

Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by Judges.

The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent. However, if a duty of confidence applies and it's within the 'reasonable expectations' of a patient that information will be shared, then this is not a breach of common law. For example, a paramedic arrives at a patients address and discharges the patient to a hospital, then it is within the 'reasonable expectation' of the patient to share data to the hospital to deliver healthcare services to the patient.

In our use of health and care information, we satisfy the common law duty of confidentiality because:

- you have 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 support from the Secretary of State for Health and Care following an application to the Confidentiality Advisory Group (CAG) who are satisfied that it isn't possible or practical to seek consent;
- we have a legal requirement to collect, share and use the data;
- for specific individual cases, we have assessed that the public interest to share 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). This will always be considered on a case-by-case basis, with careful assessment of whether it is appropriate to share the particular information, balanced against the public interest in maintaining a confidential health service.

.

How do you know your records will be kept confidential?

All NHS organisations have a legal duty of confidence to their patients and Data Protection legislation further defines how we can collect and handle personal information. The NHS also has an additional set of guidelines, known as the Caldicott principles, which apply to the use of patient information. All NHS organisations are required to appoint a Caldicott Guardian to ensure patient information is handled in accordance with legal and NHS regulations and the Caldicott Guardian for the London Ambulance Service is the Medical Director.

When we pass on any information, we will ensure that the recipient is aware that it must be kept confidential and secure.

How do we store your personal information?

Information is held for specified periods of time as set out in the Trust's Records Management and Information Lifecycle policy which accords with NHSX Records Management Code of Practice

We retain medical records for 25 years including clinical details obtained via 999 and 111 calls made by adults. Other records that may contain information about you are kept for varying lengths of time.

Records containing confidential information are destroyed in accordance with the Trust's Waste Management policy, paper records (including photographs, film, fiche and disks) being shredded, computer equipment having their drives security wiped, electronic devices having all data deleted and set to factory default, USB's having all drives security wiped, magnetic media data cartridges/cassettes having magnetic degaussing.

Data Sharing

The sharing of information has always happened (to a lesser degree) with paper processes but electronic systems are allowing us to share more relevant information about you amongst your Direct Care Team helping them to be more efficient and support theirs and your decision making on your care.

All of the people accessing and sharing your information (your Direct Care Team) will have some form of direct interaction with you otherwise they will not be accessing your information.

The reason they want to access your information is that this can improve the quality of care that you receive from them. Imagine the information or data that is held about you are pieces of a jigsaw and these pieces are held on different systems by the providers of your care.

If one of your Direct Care Team wants to make a decision on the best course of action for you, the more pieces of the jigsaw they have, the more they can know about you and your history of care and therefore they can make the most appropriate decision based on you and your needs.

We routinely collect information from the initial contact when we receive a call in the 999 Emergency Operations Centre (EOC) through to completing an electronic patient record (EPR) with information about the patient and care we provide, when we attend an incident. Some of this information goes on to form part of the Ambulance Data Set (ADS).

If a patient is transferred from ambulance services to the care of an Emergency Department, information within the Ambulance Data Set is subsequently linked with key information collected in Emergency Departments as part of the Emergency Care Data Set (ECDS).

The purpose of this is to fully understand the patient's journey from the ambulance service to other urgent and emergency healthcare settings. This will enable clinicians, ambulance services and the NHS to learn from patient journeys and further improve the care they provide in the future.

Data collected by ambulance services and emergency departments is securely linked and transferred to us. Data collected as part of the Ambulance Data Set is shared with NHS Digital* – a section of NHS England specialised in data and IT systems – where it is linked with key relevant information in the Emergency Care Data Set and securely returned to us.

This linked information includes a unique number generated by us during the initial 999 call, as well as a unique vehicle reference which will help us re-identify the original care record for the incident and the patient.

Appropriate access to this information will enable us to help develop the skills of our clinicians to improve the care they provide and support us in delivering service improvements to improve patient experience.
Patients will be able to opt out from this process if they so wish and data about their emergency care will remain with the ambulance service and / or the Emergency Department. To opt out of this process, please see the section entitled National data opt-out below.

For more information about the National Data Opt-Out, please visit https://www.nhs.uk/your-nhs-data-matters/

The lawful basis for the ambulance service to process this information under UK General Data Protection Regulation (UK GDPR) is Article 6 (1)(e) – "…exercise of official authority" and for processing special categories (health) data the basis is: Article 9(2)(h) – '…health or social care…' of the UK GDPR Regulations.

For the data collected by ambulance services (ADS) to be linked with relevant data items collected at Emergency Departments (ECDS) the lawful basis is the Sections 254(1), (3), (5) and (6), section 260(2)(d), section 261(2)(e) and section 304(9), (10) and (12) of the Health and Social Care Act 2012, as per the Ambulance Data Set

To lawfully process information in the manner described, NHS England on behalf of ambulance services have obtained a section 251 approval, as required by the NHS Act 2006 and Health Service (Control of Patient Information) Regulations 2002. This provides a legal basis for patient information to be processed for these purposes.

NHS Digital officially merged with NHS England on 1st Feb 2023, therefore the organisation previously known as NHS Digital is legally known as NHS England and data held by NHS Digital is now held within NHS England.

The Organisations involved in your Direct Care Team

The local organisations involved in your Direct Care Team include any clinician across London with a legitimate relationship to you and the right level of access to view your record.

How it works

Data sharing securely connects different medical and care computer systems together. When your record is requested by an authorised system user, the system collects the information from different systems and shows the information to the requestor. None of the information it collects is stored and none of it can be changed. Because it collects the information only when it is needed, the information is always accurate and as up to date as possible.

Before any information is collected or displayed to a care professional, they must be involved in your individual or direct care. Not everyone can see your shared data, nor should they. It will only be accessed by the people involved in looking after you directly. The Fair Processing Programme uses the secure NHS network to retrieve the information that has been approved to be shared with that care setting and displays a read only view for the care professional to use to support the delivery of care at that specific point in time.

No information is stored or saved within the or the care setting from where it is accessed so there is no need to worry about what could happen to your information without your knowledge or permission. There are two major ways that Data Sharing is taking place in London.

1. **The Summary Care Record** – The Summary Care Record contains information about your allergies, medications and reactions you have to medications, so that in an emergency or when your GP practice is closed this information is available so that you can be cared for. This is a national programme for sharing your information. For more information, please see the section below and go to www.nhscarerecords.nhs.uk.

2. **OneLondon Care Record** – This is a London wide programme which shares information about you to better support your direct care. All organisations involved in your direct will be able to access only those areas of your record that are relevant to the particular aspect of your care. These will include your GP, Acute Hospital, Local Authorities and others. A comprehensive list of these organisations is provided at www.england.nhs.uk/london/our-work/

Permission to View the Summary Care Record

London Ambulance Service NHS Trust (LAS) provides timely accident and emergency care throughout the London region. To ensure we deliver the best possible patient care to those interacting with our service, LAS have made a change so that our Paramedics, clinicians and staff that work in a clinical setting treating or assessing patients will be able to access your NHS Summary Care Record (SCR) prior to their interaction with you.

This is to support timely, effective, informed clinical decision making, to ensure you receive the very best patient care.

What is the Summary Care Record?

The Summary Care Record (SCR) is a national database that holds electronic records of important medical information about you such as current medication, allergies and details of any previous bad reactions to medicines you may have had. The SCR is created automatically from your GP medical records and whenever your GP record is updated, the changes are synchronised to your SCR. For more information, see Summary Care Records - information for patients.

Some patients, including many with long term health conditions, have previously agreed to have Additional Information shared as part of their SCR. This additional information includes information about significant medical history (past and present), reasons for medications, care plan information and immunisations. You can talk to your GP practice about opting out of including Additional Information about long term conditions, care preferences or specific communication needs.

What change has been made?

Across the wider NHS in England, health and care staff would normally ask you for your Permission to View before looking at your SCR. However, this can create a barrier to the access to vital information to support your care in the time critical situations in which LAS delivers care. LAS have therefore made a change to remove the need to ask for your Permission to View before looking at your SCR when you are in contact with our service.

When would LAS review your Summary Care Record?

LAS staff use their clinical judgement to help decide where access to your SCR would help your care. There are three situations in which we may review your Summary Care Record:

1. A Paramedic or clinician is on the way to a patient who needs emergency or urgent care and whilst being driven to the scene, the Paramedic or clinician reviews the patient's SCR to gain a clinical understanding of the patient before arrival at scene to enable them to deliver the immediate urgent critical care that the patient needs.

2. When you call 999 for help, sometimes a clinician at our Clinical Support Desk will review your case more closely to make sure you get the right care. They will look at

your call notes and your Summary Care Record (SCR), which contains important information about your health. Then, they will call you back to make sure you receive the best possible care and response.

3. For patients who contact emergency services frequently, authorised members of the Frequent Caller (FC) team may review the Summary Care Record to help understand the patient's medical history, existing care plans, medications, allergies, or safeguarding concerns. This access supports coordinated care planning, helps identify unmet needs, reduces unnecessary or inappropriate use of emergency services, and ensures that any risks are identified and escalated appropriately. Access is read-only and used only where necessary to support patient safety and effective care.

Who can see my Summary Care Record in LAS?

Only authorised, professional healthcare staff who are involved in your direct care can have access to your SCR. Your SCR will not be used for any other purposes.

These staff:
• Need to have an approved authenticator (such as a smartcard or biometric log in via an iPad
• Will only see the information they need to inform your care.
• Will have their details recorded every time they look at your record

What if I do not want my Summary Care Record to be shared?

The purpose of the Summary Care Record is to improve the care that you receive, however, if you don't want to have an SCR, you have the option to opt out. If this is your preference, please inform your GP or fill in an SCR patient consent preferences form and return it to your GP practice.

What if I do not want my data to be shared for research and planning purposes?

Your NHS health records contain a type of data called confidential patient information. This data can be used to help with research and planning. You can choose to opt out of sharing your confidential patient information being used for research and planning, and you can change your choice at any time. Find out how to make your choice here

Data Sharing – Key Questions

Why do you need to share my information?

Data sharing will provide health and social care professionals directly involved in your care access to the most up-to-date information about you.

This allows the professionals caring for you to more fully understand your needs. Information is already shared by phone and paper records, data sharing simply allows this to happen more efficiently. It does this by sharing appropriate information

from your medical and care records between health and social care services involved in your care.

Can anybody see my records?

Definitely not. Only care professionals directly involved in your care will see your personal care information through data sharing.

How do I know my records are secure?

All staff must respect your privacy and keep your information safe. Your information is stored on secure computer systems connected on a private health and social care network.

Can I access my records?

Yes. Under UK GDPR you can request access to all information that organisations hold about you. Please click on the link below to make a request:

https://www.londonambulance.nhs.uk/talking-with-us/making-requests-for-the-records-we-hold/

Can I object to my records being shared?

You can object to your information being shared by talking to your providers of care. For direct care the people viewing your records are the people directly looking after you and are doing so to give you the best quality care they can.

If you do however still want to object, please contact the organisation who holds the records you do not want to be shared. It is worth noting that not sharing vital information about you with other organisations involved in your care could affect the quality of care that you receive and there may be circumstances where your objection may not be upheld.

For example:

- If it is in the public interest for data to still be shared. For example if there is a safeguarding issue, or in the case of a mental health patient who might be at risk from harming themselves or a member of the public;
- If clinical care cannot be provided. For example, in referring a patient to hospital and data needs to be shared for the hospital clinician to do their job properly. In this instance obviously the patient can then choose not to have the treatment and therefore not have their data shared.
- If systems are not well developed enough to not share the information. For example, GP Systems are relatively well developed and can handle objections a lot more easily than other providers but they still may be asked not to share something which the system cannot do. In this instance points 1 and 2 above would apply.

What information will be shared?

Your shared record will contain a summary of your most up-to-date, relevant health information which includes things such as:

- Your recent diagnosis and test results;
- What allergies you have; what medications and treatment you currently receive;
- Any Current or Past (and significant) illnesses Encounters and Referrals.

Can everybody see everything on my medical and care records?

No. We are working very carefully, supported by health and social care professionals, to make sure only relevant information is shared into specific care settings.

Can my records be accessed by health and social care professionals outside of my borough?

Yes, they can but only with other professionals who are caring for you directly. On top of the programmes mentioned above there is also the Summary Care Record which is a national programme and as such means that it is available to care organisations outside of these boroughs (but again only for direct care purposes).

The Summary Care Record contains important health information such as:

- Any prescription medication a patient is taking
- Any allergies a patient may have
- Any bad reaction to any medication a patient may have previously had

More information about the Summary Care Record can be found at www.nhscarerecords.nhs.uk. If you have any queries or want to know more about data sharing or our fair processing, please contact your local provider that holds the information you wish to discuss.

Fleet Management Systems – Fleetwave

Fleetwave is a cloud based solution used by the London Ambulance Service fleet team for the day-to-day management of our fleet, from acquisition to disposal – including regulatory compliance and auditing. Key features include asset management, maintenance management, incident reporting, and management of Road Traffic Collision (RTC)/insurance claims.

The solution holds some personal information of our staff and third party information being processed as part of a RTC. Information is stored in the cloud on United Kingdom based servers and is transferred outside of the United Kingdom. Personal data on the system are accessible by the fleet admin for the purposes of insurance claims. The legal basis for the processing of this information is subject to the requirements of UK General Data Protection Regulation “UK GDPR” under, Article 6(1)(e), Article 6(1)(f).

- The relevant categories of personal data include – Name, address, email address, date of birth, staff payroll number and driving licence
- Recipients, sources or categories of recipients of the data – any sharing or transfers of the data will be shared with our third party insurers; QBC, Turnamms.
- Automated decision making - no automated decision making and profiling will be made.
- Retention period for the personal data – data will be kept throughout the cycle of the claim, after such time, all the information collected and processed for the purposes of claims, will be destroyed after the expiration of the data retention period.

Your Rights over Your Information

Your right of access - You have the right to ask us for copies of your personal information we hold about you, please click on this link: **https://www.londonambulance.nhs.uk/talking-with-us/making-requests-for-the-records-we-hold/**
For further details regarding Subject Access Requests, please click this link which connects you to the NHS England website: subject access request.

Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete. If you wish to contact about your records in this respect please do so at: londamb.staffsubjectaccessrequests@nhs.net
For further details regarding your rights to rectification, please click this link which connects you to the NHS England website: rectify personal information.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances. In general medical records can be corrected but have to be maintained.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

Your right to object to processing - You have the right to object to the processing of your personal information such as direct marketing or automated in certain circumstances.

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, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us at londamb.patient.experiences@nhs.net if you wish to make a request.

Information Shared with the Infected Blood Compensation Authority (IBCA)

If you have made a claim for compensation through the Infected Blood Compensation Authority (IBCA), London Ambulance Service NHS Trust may provide IBCA with relevant information from your medical records to support your claim. You can read more about how IBCA uses your information in their privacy notice (available at: https://ibca.org.uk/privacy).

National data opt-out

We are applying the national data opt-out because we are using confidential patient information for planning or research purposes

The information collected about you when you use health and care services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

- improving the quality and standards of care provided
- research into the development of new treatments
- preventing illness and diseases
- monitoring safety
- planning services

This may only take place when there is a clear lawful basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential health and care information is only used like this when allowed by law.

Whenever possible data used for research and planning is anonymised, so that you cannot be identified and your confidential information is not accessed.

You have a choice about whether you want your confidential information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt out your confidential information will still be used to support your individual care.

To find out more or to register your choice to opt out, please visit www.nhs.uk/your-nhs-data-matters.

You can change your mind about your choice at any time.

Data being used or shared for purposes beyond individual care does not include your data being shared with insurance companies or used for marketing purposes and data would only be used in this way with your specific agreement.

The Trust use of Cookies

Our website sometimes places small data files on your computer called ‘cookies’. Cookies are tiny files, which automatically download to any computer or hand held device you use whenever you go to a website. They’re designed to make your visit quicker, easier and better. A ‘cookie’ is a very small text document and cannot harm your computer, or pass on computer viruses. Most big websites use cookies as they can be useful and can:

- remember your information and settings so that you don’t have to fill it in each time you visit a new page
- let you move between pages on a website efficiently, or
- measure how you use the website, so that we can improve it to make sure it meets your needs. For example it may tell us the type of internet browser you use (such as Google Chrome, Internet Explorer etc.), the type of device you are using eg. smart phone, PC, Mac, or the language you are using. This means we can make sure our site works for all these different devices and settings, and improves your user experience.

We don’t use the cookies to identify you personally; they are just here to make the site work better.

How to manage and control cookies

You can choose to accept or decline cookies. Most web browsers, such as Internet Explorer, Safari, Google Chrome, automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer.

If you do not want is to place cookies on your computer or handheld device, you can change your settings to stop this. This may prevent you from taking full advantage of the website. Here is a useful site explaining how to manage cookies:

https://ico.org.uk/for-the-public/online/cookies/

This website explains how to alter your browser settings (such as Internet Explorer, Google Chrome, Safari etc.) to refuse cookies. However, if you choose to have your browser refuse cookies, it is possible that some areas of our site will not function as effectively.

How we use cookies on our site

On our site we use a few cookies, to help make your experience better.

Google Analytics

Name(s): _utma,_utmb,_utmc,_utmz

These cookies are used to collect information about how visitors use our site. We use the information to compile reports and to help us improve the site. The cookies

collect information in an anonymous form, including the number of visitors to the site, where visitors have come to the site from and the pages they visited.

Click here for an overview of privacy at Google

Site Session Cookie

Name: ASP.NET_SessionId

This cookie is essential for the forms on the site to operate. For example, when you fill in a form to give us feedback, thank our staff, register for an event or make a complaint.

YouTube

Name: VISITOR_INFO1_LIVE

This cookie is essential for the forms on the site to operate. For example, when you fill in a form to give us feedback, thank our staff, register for an event or make a complaint.

Google Maps

Names: NID,PREF

These cookies are set and used by pages with embedded Google maps. These maps show our locations and locations of events you may wish to attend.

To learn more about cookies and how to manage them, visit AboutCookies.org.

Information collection

If you register with the website, or if you fill in a form on the website, you may be asked to provide information about yourself (including your name and contact details).

We may also collect information about your usage of this website as you and others browse and use our website, as well as information about you from messages you post to the website and emails or letters you send to us.

Use of the information we collect

Your personal information will be used for several general purposes, including: providing information that you have requested, handling your enquiries, personalising your experience on the website, providing access to some areas of the website, and keeping you up-to-date with services which may be relevant to you where you have indicated that you wish to receive this information.

If you have consented to receive additional service updates, we may also provide other information which we think you may find of interest, such as training events. In these circumstances, The Trust will contact you by your preferred method of post, telephone or fax, as well as by email. You are given the opportunity to opt-out of receiving this information at the appropriate section of the website when you register your details. If you no longer wish to be contacted in the future by us using details obtained from this website, please contact londamb.press.office@nhs.net.

Webserver log files

IP addresses are used by your computer every time you are connected to the Internet. Your IP address is a number that is used by computers on the network to identify your computer. IP addresses are automatically collected by our web servers so that data (such as the web pages you request) can be sent to you.

Webserver log files are used to record information about our site, such as system errors. The Trust also uses log files to monitor site traffic. Log files do not contain any personal information or information about which other sites you have visited.

Security

Unfortunately, the transmission of information via the Internet is not completely secure. Although we employ security measures to protect the information provided by you, the Trust cannot guarantee the security of your data transmitted to our site and any transmission is at your own risk. Once we have received your information, we will use appropriate security procedures and features aimed at preventing any unauthorised access, unlawful processing, accidental loss, destruction or damage

Links to external sites

This website contains links to other websites, both those of government departments and of other organisations. This Privacy Notice applies only to this Trust, so when you are moving to another site which collects personal information you should always read the Privacy Notice relating to that organisation.

How do I complain about the LAS service?

Our Patient Experiences team is your first point of contact if you would like to make a complaint or raise a concern about our service. Please click on the following link:

https://www.londonambulance.nhs.uk/talking-with-us/enquiries-feedback-complaints/

How do I report a personal data breach?

If you have any concerns about our use of your personal information, you can make a complaint to us at:

Information Governance team
London Ambulance Service NHS Trust
220 Waterloo Road
London SE1 8SD

Email: londamb.ig@nhs.net

Following this, if you are still unhappy with how we have used your data, you can then complain to the ICO.

The ICO's address is:

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

Helpline number: 0303 123 1113

ICO website: https://www.ico.org.uk

Date of last review

20th October 2026 - next review 1st December 2026