Privacy Notice – Employment Records

During the course of its employment activities, South East Coast Ambulance Service NHS Foundation Trust collects, stores and processes personal information about prospective, current and former staff.

This Privacy Notice includes applicants, employees (and former employees), workers (including agency, casual and contracted staff), volunteers, trainees and those carrying out work experience.

We recognise the need to treat staff personal and sensitive data in a fair and lawful manner. No personal information held by us will be processed unless the requirements for fair and lawful processing can be met.

What types of personal data do we handle?

In order to carry out our activities and obligations as an employer we handle data in relation to:

- Personal demographics (including gender, race, ethnicity, sexual orientation, religion)
- Contact details such as names, addresses, telephone numbers and Emergency contact(s)
- Employment records (including professional membership, references, and proof of eligibility to work in the UK and security checks)
- Recruitment information
- Vaccination uptake information – Flu data
- Occupational Health information
- Compliance with Driver Check standards
- ID documentation
- Correspondence sent and received using any Trust communication systems in relation to your employment activities. This includes personal data sent or received using these systems.
- Bank details
- Pension details
- Medical information including physical health or mental condition (occupational health information)
- Information relating to health and safety
- Trade union membership
- Offences (including alleged offences), criminal proceedings, outcomes and sentences
- Employment Tribunal applications, complaints, accidents, and incident details
- Foundation Trust Membership

Our staff and contracted providers are trained to handle your information correctly and protect your confidentiality and privacy.

We maintain high standards, adopt best practice for our record keeping and regularly check and report on how we are doing. Your information is never collected or sold for direct marketing purposes.

The Trust does not process information abroad. However, there may be ad-hoc occasions where working abroad is agreed for a short timeframe in line with Trusts Agile Working Policy.

The Trusts Car Club and Hire Travel scheme (Enterprise) holds minimal personal data within the USA. See **Car Club and Hire Travel** section below for further information.

What is the purpose of processing data?

- Staff administration and management (including recruitment, contract, payroll, and performance)
- Fulfilling your duties and responsibilities
- Pensions administration
- Mandatory compliance standards
- Business management and planning
- Accounting and Auditing
- Accounts and records
- Crime prevention and prosecution of offenders
- Education
- Health administration and services including Occupational Health
- Information and databank administration
- Sharing and matching of personal information for national fraud initiative

We have a legal basis to process this as part of your contract of employment (either permanent or temporary) or as part of our recruitment processes following data protection and employment legislation.

Optima Health

Occupational Health is a specialist branch of medicine that focuses on the physical and mental wellbeing of employees in the workplace.

Optima Health is an externally contracted Occupational Health provider for South East Coast Ambulance Service (SECAmb). This service is used by SECAmb managers to refer a member of staff, Occupational Health team members receive referrals and manage delivery of the Occupational Health workstream.

Information is provided by SECAmb and held by Optima. SECAmb is the Data Controller and Optima Health are the Data Processor. Optima are registered with the Information Commissioners Office and have a Data Protection Officer. The MyOHportal system is used by Optima Health for delivery of Occupational Health Services to customers. Full technical and IG assurance has been completed.

The aim of occupational health is to prevent work-related illness and injury by:

- encouraging safe working practices;
- ergonomics (studying how you work and how you could work better);
- monitoring the health of the workforce;
- supporting the management of sickness absence.

Occupational Health receive and process the following information.

- Names, address, date of birth, email, telephone
- From manager – referral questions, absence record , any other concerns with consent
- From individual with consent– underlying health conditions, how this impacts them , home circumstances so that an assessment can be carried out . This would be kept as part of the medical record under confidential circumstances within their portal.
- If further medical evidence is required, we would write to GP with the individuals consent to gain this . This would be scanned into cohort and kept within their record . Any paper report from the GP would be destroyed.
- From an individual after needlestick – circumstances of incident, protection status, blood tests to confirm if individual is protected.
- Occupational Health also receive completed pre-placement questionnaires from candidates going through the recruitment process.

This data is needed to ensure that SECAmb is meeting its duty of care as employers for its workforce, enabling staff's health and wellbeing to be supported by management and an external Occupational Health third party.

LEGAL BASIS FOR PROCESSING: UK GENERAL DATA PROTECTION REGULATION

Consent is the legal basis.
Article 6 (1) (a) "the data subject has given consent to the processing of his or her personal data for one or more specific purposes";
Article 9 (2) (a) "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes".

Audit Compliance and Outcome Information

As part of the Trusts Clinical Audit function the clinical audit department measures the documentation of patient care against agreed national and local standards. Some conditions (STEMI, Sepsis, Stroke and Cardiac Arrest patients) are reported nationally and SECAmb is benchmarked against other Ambulance Trusts.

Feedback to management teams and individual clinicians highlighting areas of good practice and areas required for improvement is essential. This ensures that managers and clinicians alike are aware of their current performance which is integral to improving performance and patient outcomes.

From the 5 December 2022 a new process will be trialled. This will involve disseminating existing information processed by the clinical audit team to various staff within Operations. The purpose of processing is to provide feedback in relation to patient survival and audit outcomes.

This resulting information relating to patient outcomes will be in an anonymised format. It will not be used for performance management but for individual clinician learning.

The agreed process for feedback will be;

1) Through a dashboard using aggregated statistics that will be available at OUM level.
2) Through a table at OU level, the OU's compliance will be broken down to incident level.
3) Compliant Audits, Survival and Confirmed Stroke - Through direct feedback from clinical audit to clinicians. This will be via a letter (signed by the medical director).
4) Through cardiac arrest skills feedback. This will be conducted by the critical care paramedics to the clinicians through verbal feedback and a Code-Stat Report.
5) Non-Compliant Audits – The clinical audit department will email the OTLs, who will speak directly with the clinicians. Within the email there will be clear instructions as to how to challenge an audit compliance result

A full Data Protection Impact Assessment has been completed for this processing activity. A copy of which is available on request via clinical.audit@secamb.nhs.uk

Data Subject Access Requests (DSARs)

Under Article 15 - Right of Access of the UK GDPR individuals are entitled to request a copy of the personal data held about them by an organisation. SECAmb retains full ownership of data and is the data controller.

The Trust has an approved DSAR policy and process in place which provides information regarding the process and portfolio contacts. Any DSAR relating to Optima Health should in the first instance be referred to the Wellbeing Team.

Right to Rectification

Under Article 16 of the UK GDPR individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

The Trust must manage requests for personal information to be rectified or forgotten. It has an approved Data Subject Access Request policy which also references requests which fall under these conditions of processing.

Any requests relating to the 'right to rectification' must be initially referred to the Head of Information Governance / Head of Legal Services.

Right to Erasure

Under Article 17 of the UK GDPR individuals have the *right to request* that personal data is erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances

The Trust must manage requests for personal information to be rectified or forgotten. It has an approved Data Subject Access Request policy which also references requests which fall under these conditions of processing.

However, there are exemptions to such and the Right to Erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information.
- to comply with a legal obligation.
- or the performance of a task carried out in the public interest or in the exercise of official authority.
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise, or defence of legal claims

Requests relating to the 'right to be forgotten' must be initially referred to the Head of Information Governance / Head of Legal Services.

For further information please access the Wellbeing Hub Privacy Notice which is located on the Zone.

Contact information

You may contact the team at wellbeinghub@secamb.nhs.uk or alternatively write to us at:

Nexus House,
4 Gatwick Road,
Crawley RH10 9BG

Alternatively, you can call us between 9.00am and 5.00pm, Monday to Friday, (not including Bank Holidays) on 0300 1239 191.

Flu Vaccination data

As a Trust SECAmb is set an annual CQUIN target for uptake of staff influenza (flu) vaccinations. Flu vaccination is voluntary and offered to all staff with the Trust mandated to record and report uptake.

Vaccination uptake is recorded through the completion of an MS Teams form by the data subject. The purpose of processing is to ensure that the Trust has an accurate record of its annual flu

vaccination uptake with minimal data processed. Our adherence to data protection is clearly explained within the form. All information is treated in a confidential manner.

Completed forms are retained securely within the IPC team with strict role-based access controls in place. This information is only accessible by the IPC team and will be retained until March 2023. Following which the data will be securely destroyed with certificates of destruction completed.

Analytical uptake figures are provided at a national and internal level. **No personal data is imparted.** Internal reporting includes analytical figures at a directorate and OU level.

National Immunisation Vaccination System (NIVS) – Staff Data

The National Immunisation Vaccination Service (NIVS) provided by NHS England and NHS Improvement is used to record the vaccination details of healthcare workers. The IPC team use this system to record flu vaccination uptake.

This system delivers a centralised data capture tool for clinical teams delivering the seasonal flu immunisation. Vaccination event data will be fed back to GP clinical systems.

The NIVS system processes minimal information in line with the purposes of processing.

Data Sets:
1. NHS Number
2. Forename
3. Surname
4. Postcode
5. Gender
6. DOB

The National Data Opt Out provision does not apply to this data processing

COVID related data

During COVID the Trust conducted its own internal vaccination programmes which were led and delivered by the Covid Management Team. All of these involved the processing of personal sensitive data. The First General Control of Patient Information (COPI) Notice issued in March 2020 expired on the 30 June 2022. This notice allowed the sharing of COVID related data during the pandemic whilst satisfying the Common Law duty of Confidentiality, although a legal basis under data protection legislation was still required.

With the expiry of COPI organisations have been requested to review their processing activities and the retention / or further processing of COVID related data. Discussions remain ongoing at a national level in relation to data processing. As data controllers' organisations have been tasked with reviewing the data they have collected, data retention and whether there is a legal basis for continuing to undertake and process such information moving forward.

Currently, all COVID related data processed relating to the vaccination programme and monitoring of COVID is securely held with strict role-based access controls in place.

This information will not be further processed without an agreed formal legal basis but will be temporarily retained due to the forthcoming COVID public inquiry.

Car Club and Hire Travel

The Trust uses the 'Enterprise Rent – A – Car' or 'Enterprise Car Club' for Employees who have previously used their own personal vehicle for business travel. This arrangement applies to all Trust employees currently based at HQ Crawley, staff on courses facilitated by Clinical Education and staff employed at other Trust locations who do not have access to a Trust lease car and would otherwise use their own private vehicle.

The company engaged with this scheme, Enterprise Rent-A-Car or Enterprise car club is registered within the USA. Therefore, the following information below is imparted to ensure that the Trust is open and transparent with its Employees.

Information collected by Enterprise Rent-A-Car or Enterprise car as part of the scheme is currently held within the USA, and outside of the EEA. Enterprise are aware of the decision made by the European Court of Justice (Schrems II) in July 2020 which resulted in the invalidation of the E.U.- U.S. Privacy Shield program. In response, they have confirmed the following:

The court in Schrems II upheld the validity of the EU-approved model contract clauses but encouraged companies that rely on the model clauses to confirm additional safeguards are in place to comply with the contractual requirements.

Enterprise Rent-A-Car UK Ltd has relied on both Privacy Shield and the approved model clauses to transfer data outside the UK. While the Schrems II decision invalidated Privacy Shield, Enterprise Rent-A-Car UK Ltd continues to satisfy UK legal requirements to transfer data through the use of approved model clauses to Enterprise Holdings, Inc (EHI), its parent company in the U.S. EHI is not an electronic communication service provider or network provider that the U.S. Government compels to provide information, facilities, or assistance in conducting bulk surveillance, and EHI has never voluntarily provided such information, facilities, or assistance.

In accordance with the mandate of the Schrems II decision, Enterprise is conducting additional due diligence (including risk assessments) to determine whether additional safeguards or supplemental measures are necessary to maintain compliance with the General Data Protection Regulation. This is an evolving situation, and we are carefully monitoring new developments, guidance and recommendations by the European Data Protection Board and the European Commission. The privacy and security of our customer data is of utmost importance to us and are committed to ensuring we abide by our global privacy policy and legally approved mechanisms for transferring data outside the UK

Enterprise hold a: Privacy Notice which specifies that personal information may be used for / shared for

- Marketing purposes:
- Rental transactions:
- Customer service-related queries:
- Disputes & law enforcement:
- Subsidiaries:
- Franchises:
- Service Providers and Business Partners:

Enterprise provides the provision for Employees to 'opt-out' of having their information shared for direct marketing purposes should they wish to do so. This is detailed within their Privacy Notice as below:
https://privacy.ehi.com

The Trust also holds a compliant Pilot Car Club and Hire Travel Policy and Procedure which has been reviewed and approved.

Automated Driving Licence system – Driver Check

In order for the Trust to remain compliant it needs to ensure that staff members driving licences are checked on a quarterly basis. This provides assurance that individuals are legal to drive for and on behalf of the Trust.

This process has now moved to a third-party company (provider) called DriverCheck who will provide an automated streamlined system, digitalising the process. Driver Check are a 3rd party processor, registered with the Information Commissioners Office (ICO). They are compliant with data protection legislation and conform to all ISO27001 standards which include the interrogation / processing of personal data away from the office. Data is held in Microsoft Azure Cloud located within the UK

Driver Check will not use / share the data for any other purpose other than driving licence checking – this is a key contractual requirement within DriverCheck's DVLA agreement. The only exception being if there is a requirement in law.

Data processed includes:

- Employee number,
- Name,
- Address,
- Date of birth
- Driving licence number
- DVLA D/L returned data (points, endorsements, date of offence, conviction, entitlement to drive, expiry dates, categories and photocard, address information).
- Base location
- Organisation email address
- Points,
- Endorsements,
- Date of driving offence,
- Driving conviction,
- Entitlement to drive.

This is the minimum data set needed to provide information to the DVLA. This processing is proportionate and not excessive and is needed by the Trust in order to check legal compliance. Each staff member will be sent a registration email which will require them to enter in the pieces of data to complete the check. Permission is provided for a 3-year period.

Consent is explicit, as the staff member is sending their information so that they can have their license checked. This is a condition of their employment, to which they have signed a contract. Staff will provide their consent by completing a form and authorising a check to be completed. This is referred to as “Fair Processing declaration”.

UK General Data Protection Legislation

Consent is explicit, as the staff member is presenting their information as part of the condition of their employment, to which they have signed a contract

Article 6 (1) (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

No Special Category Article 9 data is processed.

Driver Compliance checks via Selenity

As an organisation SECAmb must ensure it complies with its driver compliance and insurance requirements. This requirement is completed individually by Trust employees who upload their personal information for the purposes of processing and claiming expenses.

The information will be maintained by the individual uploading their insurance information onto Selenity. Any change to this information will be the sole responsibility of the staff member to inform the trust

In order to achieve this SECAmb uses the driver compliance module within the Selenity e-expenses solution to validate insurance information. Selenity is the data processor. Only relevant information is processed using a minimum data set in line with Trust policy

Vehicle road compliance is automatically checked when a car registration is entered onto the system. It is checked for valid tax and MOT. However, this system does not hold individual driver license information, this information is retained within GRS Driver Check and is only accessible by SECAmb employees with the appropriate role-based access controls in place.

The processing of this data is needed to ensure the Trust meets its contractual obligations under Agenda for Change.

Personal information processed:

- Name and address
- email address (work)

Legal basis for processing personal information:

Article 6 (1) - (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

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

Identity compliance – Trust ID

Trust ID is an electronic cloud-based scanning solution that allows for the verified checking of NHS Employment Check Standards. This is a mandatory check which all Trusts must carry out in the recruitment and ongoing employment of all staff, whether permanent, temporary or volunteers.

The purpose of processing the data is to ensure that new employees are onboarded correctly and ensure that existing employees are effectively verified against the NHS Employers pre-employment and on-going checking standards.

Trust ID scanning technology will enable the Trust HR team to demonstrate compliance with the NHS Employment Check Standards for Right to Work and identity validation by using the scanning system. Automatic reassurance is provided to the CQC and the Home Office.

Right to work data will be processed through the Trust ID scanning system. The data will remain on the Trust ID system for 7 days. The Trust will download the data into the Trac system daily and updated into the SharePoint electronic system.

After 7 days the data on Trust ID will be automatically deleted. At the end of the recruitment process successful candidate's data will be downloaded from the system and saved locally within the SECAmb infrastructure.

Legal basis for processing personal information:

Article 6 (1) (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

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

TRAC

TRAC is a recruitment system which allows for the integration of the majority of recruitment processes into one streamlined system by ensuring that the process for administering new starters is in one central location. This is an established recruitment system, widely used within the NHS and part of the NHS Procurement framework

The purpose of processing personal data via TRAC is to ensure that new employees are onboarded correctly. The collating of data will now be processed via TRAC, and all data will remain within the TRAC system until the end of the recruitment process. At the end of the recruitment process the successful candidate's data will be downloaded from the TRAC system and saved locally within SECAmb's infrastructure with appropriate role-based access controls in place.

Consent is explicit, as the potential employee is sending their personal information voluntarily in order that they can gain employment.

SECAmb is the Data Controller and TRAC is the Data Processor

How can you access your employee records?

Data Protection legislation gives you a right to access the information we hold about you in our records. Details of the information you are requesting are needed, this should include full name, the type of information this relates to and the approximate date.

The Trust will provide your information within one month from receipt of the request. There is no fee payable for this service.

Please email us at hr.sar@secamb.nhs.uk

Or write to us at:

South East Coast Ambulance Service
Ambulance Headquarters
HR Directorate – Data Subject Access request
Nexus House,
4 Gatwick Road,
Crawley
RH10 9BG

ESR Self Service (Limited Access)

All Employees will have a unique username and password to log onto, this provides staff members to:

- View and amend personal information including, address, phone numbers, bank details and emergency contacts
- View payslips, P60's and total reward statements
- View and amend Equality and Diversity information including, religious beliefs, sexual orientation, and disability information

SECAmb Foundation Trust Membership

Foundation Trusts are different from standard NHS Trusts. They have freedom to decide locally how to meet their obligations and they are accountable to local people and staff who can become members and governors. As a Foundation Trust SECAmb has a statutory duty to ensure that its membership is representative of the organisation and the areas it serves.

Under contract of employment a staff member is a Foundation Trust member unless they advise that they wish to 'opt out'.

FT membership is free and crucially it means you can vote and or even stand in Staff Governor Elections. Staff Governors represent you at our Council meetings and make sure the Trust is acting in the best interests of its staff, volunteers, and patients. The Trust plans to use the National Health Service Act 2006, as our lawful basis for processing membership data because there is a statutory requirement to do so, and it is exercising its official authority as a public body.

Should you decide to 'opt out' of Foundation Trust membership please contact the Membership Office as follows:

Email: ftmembership@secamb.nhs.uk
Tel: 0300 123 9180
Mobile/SMS: 07770 728 250

Postal address:
Membership Office
South East Coast Ambulance Service NHS Foundation Trust
Nexus House
4 Gatwick Road
Crawley
RH10 9BG

Trust Constitution

The Trust has a constitution, which details that the Trust shall have members, each of whom shall be a member of one of the following constituencies:

- A public constituency - an individual who lives in an area served by the Trust.
- A staff constituency - an individual who is employed by the Trust.

The Trusts constitution can be viewed online here:
http://www.secamb.nhs.uk/about_us/document_library.aspx

More information on membership can be found on our website here:
http://www.secamb.nhs.uk/get_involved/membership_zone.aspx or by emailing the membership office FTMembership@secamb.nhs.uk

Sharing your information

There are a number of reasons why we share information. These can be due to:
- Our obligations to comply with legislation
- Our duty to comply any Court Orders which may be imposed

Any disclosures of personal data are always made on case-by-case basis, using the minimum personal data necessary for the specific purpose and circumstances and with the appropriate security controls in place. Information is only shared with those agencies and bodies who have a "need to know" or where you have consented to the disclosure of your personal data to such persons.

Use of Third-Party Companies

To enable effective staff administration South East Coast Ambulance Service NHS Foundation Trust may share your information with external companies to process your data on our behalf in order to comply with our obligations as an employer.

Employee Records; Contracts Administration (NHS Business Services Authority)

The information which you provide during the course of your employment (including the recruitment process) will be shared with the NHS Business Services Authority for maintaining your employment records, held on the national NHS Electronic Staff Record (ESR) system.

Data affecting pay will also be viewable by our payroll provider, who has a legal basis to access pay relating information, to comply with our obligations to you as an employee.

In addition to this, personal information may also need to be shared with NHS partner organisations in line with compliance requirements.

For example, providing NHS Digital with an individual's name as part of the national NHS Pathways accreditation process. In such instances, the Trust will only impart information where there is a legal basis, will use minimal personal data and will ensure that this is sent securely.

Payroll Services - New contacts for Payroll & Pensions from 1 October 2021

From the 1 October 2021 the Trusts payroll and pensions provision moved across to University Hospitals Birmingham NHS Foundation Trust (UHB). Full information governance assurance has been completed.

As part of the service provision a full dedicated UHB team will be available during normal working hours (9:00 until 17:00 Monday to Friday excluding public holidays). The new contact email addresses are as follows:

Payroll general queries:
SECAMBPayroll@uhb.nhs.uk

Pension general queries:
278pensions@uhb.nhs.uk

Staff are offered a choice of telephone numbers according to the service and enquiry they need assistance with – please refer to the Pay & Conditions and Pensions pages on The Zone for these (effective 1 October 2021). **All enquiries must be directed to UHB in the first instance**,

Prevention and Detection of Crime and Fraud

We may use the information we hold about you to detect and prevent crime or fraud. We may also share this information with other bodies that inspect and manage public funds.

We will not routinely disclose any information about you without your express permission. However, there are circumstances where we must or can share information about you owing to a legal/statutory obligation.

Individuals Rights

Data Protection laws give individuals rights in respect of the personal information that we hold about you. These are:

1. To be informed why, where, and how we use your information.
2. To ask for access to your information.
3. To ask for your information to be corrected if it is inaccurate or incomplete.
4. To ask for your information to be deleted or removed where there is no need for us to continue processing it.
5. To ask us to restrict the use of your information.
6. To ask us to copy or transfer your information from one IT system to another in a safe and secure way, without impacting the quality of the information.
7. To object to how your information is used.
8. To challenge any decisions made without human intervention (automated decision making)

Please visit our website for further details on this.

Should you have any further queries on the uses of your information, please speak to the Human Resources Department or our Data Protection Officer – Caroline Smart, Head of Information Governance

Should you wish to lodge a complaint about the use of your information, please contact our Human Resources Department at:

South East Coast Ambulance Service NHS Foundation Trust
Ambulance Headquarters
Nexus House
Gatwick Road
Crawley
RH10 9BG

If you are still unhappy with the outcome of your enquiry you can write to:

The Information Commissioner,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire SK9 5AF

Telephone: 01625 545700.
Website : https://ico.org.uk/