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 and COVID 19
- Lateral Flow Testing – National reporting requirements
- 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 or processed overseas. Except for the Trust Car Club and Hire Travel scheme which holds minimal personal data within the USA.

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
- 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.

COVID - 19

Health and social care systems continue to face significant pressures under Covid-19. Health and care information is essential to deliver care to individuals, support health and social care services and to protect public health. Information is vital in researching, monitoring, tracking, and managing the ongoing outbreak, and is also used to monitor and nationally report on COVID and Flu vaccination uptake

Existing law which allows confidential patient information to be used and shared appropriately and lawfully in a public health emergency is continuing to be used. Using this law, the Secretary of State has required NHS Digital; NHS England and Improvement; Arm's Length Bodies (such as Public Health England); local authorities; health organisations and GPs to share confidential patient information to respond to Covid-19.

Any information processed or shared relating to Covid-19 will be limited to the period of the outbreak unless there is another legal basis to use the data.

Control of Patient Information (COPI Notice)

The Secretary of State for Health and Social Care issued NHS Digital with a Notice under Regulation 3(4) of the National Health Service (Control of Patient Information Regulations) 2002 (COPI) to require NHS Digital to share confidential patient information with organisations entitled to process this under COPI for COVID-19 purposes.

This legislation was implemented in March 2020 and has now been extended until 30 June 2022
https://digital.nhs.uk/coronavirus/coronavirus-covid-19-response-information-governance-hub/control-of-patient-information-copi-notice

NHS England's basis to process confidential patient information, setting aside the duty of confidence, is regulation 3(3) of the Health Service (Control of Patient Information) Regulations 2002 (COPI), which were made under section 251 of the NHS Act 2006.

COPI does not provide a blanket lawful basis to processes personal confidential data but provides a gateway for sharing and sets aside the common law duty of confidentiality. However, data protection law (GDPR and the DPA 2018) must still be complied with.

GDPR Legal Basis

For GDPR purposes NHS England's lawful basis for processing is;
Article 6(1)(e) – '…exercise of official authority…'.
Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

For the processing of special categories (health) data the conditions are:
Article 9(2)(h) – '…health or social care…'
Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems

Article 9(2)(i) – '…public health purposes…',
Processing is necessary for reasons of public interest in the area of public health,

Article 9(2)(j) – '……archiving…research…or statistical purposes…'
Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

For processing special categories (ethnicity) data the conditions are
Article 9(2)(b) – '…social protection law…' (for monitoring equality of access)
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 and social protection law

Article 9(2)(h) – '…health or social care…'
Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems

Article 9(2)(j) – '……archiving…research…or statistical purposes…'
Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

COVID – 19 testing

In circumstances where you tell us you're experiencing Covid-19 symptoms we may need to collect specific health data about you. Where we need to do so, we will not collect more information than we require, and we will ensure that any information collected is treated with the appropriate safeguards.

Data may be shared with laboratories which are government run and in the private sector under the guidance of Public Health England. This data is limited to that which is required to ensure test results can be communicated back to the individual. Normally this will be a phone number, home address and email address linked to a named individual with date of birth and where available NHS number.

COVID - 19 Test and Trace Service

Due to the COVID-19 outbreak the Trust was asked to establish a Test and Trace cell to support the Public Health England (PHE) Tier 1 contact tracing level (referred to as complex cases) of the service through the implementation of a local contact tracing policy of their employees when a staff member* is confirmed as COVID-19 positive.

*This caveat also includes CFR's, Volunteers, Contractors and Patients which the Trust has provided care to as an emergency service.

Positive cases may be identified internally or passed to the Trust via secure email from Public Health England. The Trust needs to accurately record details of confirmed or suspected COVID-19 cases and staff who may have been exposed to COVID-19 through contact with those individuals.

The information (data collection) recorded is kept to a minimum and will be held and retained in line with the NHSx Records Management Code of Practice.
**In the event of a declared outbreak by Public Health England this data will be held for an indefinite period and until all investigations are completed.*

This includes the following personal data:
1. Operating unit or department
2. Full name and address
3. Date of birth
4. Payroll number
5. Preferred contact number
6. Preferred email address
7. NHS number
8. CAD Reference (where applicable)
9. COVID-19 test location, date, and results (where required)
10. Additional notes

The information is hosted within SECAmb systems. There are defined role-based access controls in place assigned by the COVID-19 Management Team and a process to ensure the closure of system access when required. The system allows records to be altered only by authorised personnel with validations in place to ensure correct information is entered. Access to records is recorded, and fully auditable. A viewed records log can be produced if required.

PathEKS

Flu and COVID Vaccination data / Lateral Flow testing

Under COVID 19 the Trust is mandated to record Lateral Flow Testing and uptake of Flu / COVID Vaccination data. This information is reported at a national level to Public Health England and NHS England. To meet these requirements the Trust utilises a system called PathEKS. The system allows staff to access an online appointment management system through a secure booking portal. Once online individuals create a personal profile, select an appointment time and date, the system will then confirm the booking automatically via text and email based on the information provided.

This system is hosted by East Kent Hospital University NHS Foundation Trust (EKHUFT) who host and administer PathEKS. Information is held securely on their Trust servers housed within their own data centre. SECAmb is the Data Controller and East Kent Hospitals University Foundation Trust Data Team are the Data Processor

The PathEKS system will hold personal identifiable data which is required to process Lateral Flow Testing results and vaccination uptake relating to Flu and COVID, including the recent booster vaccination programme

This processing includes:
- Name
- Address
- Postcode
- NHS number
- Gender
- Employee number
  Email / Telephone number

* *Health information, specific to purpose and provided during the clinical vaccination process.*

PathEKS Vaccination information

SECAmb has administration access to review the data for attendees at the vaccination clinics, this information is needed for reporting purposes. Internal role-based access controls are in place to ensure that access is restricted to those who require this as part of their role and responsibility. This information is then used to update the National Immunisation Vaccination System (NIVS) for healthcare worker

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. From September 2021 the Trust will be utilising PathEKS which will ensure that COVID-19 and Flu vaccination data is held centrally with the correct governance controls in place.

East Kent Hospital University NHS Foundation Trust (EKHUFT) internal development team created the 'PathEKS' system. This is used as a booking portal utilised for; Staff COVID-19 Vaccination Clinic Slots (Covax), Lateral Flow and Staff Flu vaccination uptake (Flu Jab).

The system allows for staff to access an online appointment management system (PathEKS) through a secure portal. Once online they can create a personal profile, select an appointment time and date, and the system will confirm the booking automatically via text and email which eliminates the need for local in-house support.

The objective to provide a secure solution for data processing which is fit for purpose and provides the reporting functionality which is needed. The system is hosted by EKHUFT on their internal Trust servers and housed within a data centre within EKHUFT. It provides a dedicated database for SECAmb the Data Controller, with EKHUFT being the Data Processor

Access to PathEKS is restricted using locally held role-based access controls. It has the functionality to enable reports to be produced so that uptake can be monitored and reported on. Information held within PathEKS is also reported into the National Immunisation Vaccination System (NIVS) for healthcare workers. SECAmb will have administration access to review the data for any attendees at the Flu vaccination clinics. This will enable uptake and national reporting requirements to be completed.

National Immunisation Vaccination System (NIVS) – Staff Data

NHS England has commissioned and implemented a National Immunisation Vaccination Service (NIVS). This is provided by NHS England and NHS Improvement and will be used to record the vaccination details of healthcare workers.

This delivers a centralised data capture tool for clinical teams delivering the seasonal flu immunisation and is an essential component of NHS England's response to the COVID-19 pandemic. The vaccination event data will feed back to GP systems and the National Immunisations Management System (NIMS).

Information will be recorded within NIVS using minimal information

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

Data will be disseminated to NHS Digital as Data Processors on behalf of NHS England. Further information regarding the use of data can be found via the link below.
https://www.england.nhs.uk/increasing-health-and-social-care-worker-flu-vaccinations/niv-faqs/

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

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/