EUROMED SERVICES LTD T/A EUROMED AMBULANCE
Privacy Policy

Euromed Services Limited privacy policy as published in May 2018

Personal data we use at Euromed Services Limited (the company) will hold data relevant to its business activities, this as such includes contact information for companies and individuals for the purposes of contacting them with regards to bookings made by the client.

Clients data will be held in compressed zip files and only accessed by the relevant employees that require the data for the purposes it is intended to be used for.

The data held is given to Euromed Services Limited under consent of the owner at the point of contact., by completing any form requiring personal data either by email or online the owner of the data is consenting to Euromed Ambulance, Euromed Special Operations or Euromed Training & Development and its employees using and storing this data for its relevant and intended purpose.

Due to the nature of Euromed's Business activities staff will engage in activities as such that during the course of carrying out its duties may involve in depth personal data of individuals including sensitive information relating to medical conditions. This information is required to held for 7 years after the data is supplied. All information is confidential and is held in secure storage at Euromed head office. No personal patient information should be removed from the premises without the consent of the Directors.

Patient information may be shared with other medical professionals such as doctors or other NHS staff for the wellbeing of the patient and in the course of required medical treatment.

This includes, but is not limited to -

Staff Records

Full name including aliases, home address, contact telephone numbers, email address, date of birth, Next of Kin, employment history and enhanced DBS records, bank details for payroll purposes, passport details for security purposes (where required), immunisation status (clinical staff only) and driving licence details.

Patient Records

Full name and address, contact telephone numbers, date of birth, GP details, medical history including current medication and known allergies, Next of Kin, Powers' of Attorney (where applicable)

Client records (including requests for quotation)

Full name and address, contact telephone numbers, email addresses, event location(s), details of event type and attendee numbers.

Suppliers

Full name and address, contact telephone numbers, email addresses, services/equipment provided, cost information.

Others

In limited cases, names and contact details of relatives may be requested informally to help support the management of a patient.

Data Origin

Data held by Euromed Services Limited is provided by the owner of the data, for example an event organiser provides information relating to an event along with their personal information and contact details for the purpose of Euromed engaging in communication relating to the services offered for reward by Euromed Services.

The data supplied is always supplied by the owner with consent with the exception of a patient who lacks capacity to consent.

Data Sharing

Data specific to an event will be shared with the relevant staff or contractors that will require the information for them to carry out the task they are employed to do.

Patient data may be shared with medical staff from the NHS or private medical faculties for the intended purpose of patient wellbeing and treatment relevant to the patient.in this instance data will be available from both parties involved via a subject access request.

Data changes and corrections

Any data held by Euromed may be changed for the purpose of corrections by the data owner at any time.

You may be asked to provide proof of ownership of the data in question. Anyone requesting data changes must have a valid reason to do so and proof that the change is genuine.

Client records (including requests for quotation)

Euromed will do what is reasonably practical to ensure that data is collected, handled and stored in accordance with the GDPR.

In order to achieve this it will specifically ensure that where data is collected the data subject is clearly aware of the way in which this data may be used, stored and managed.

The company will ensure that access to data is provided strictly on a 'need to know' basis and that staff regularly handling data are aware of their responsibilities under the GDPR to maintain the security of this data.

The company will do what is reasonable to ensure the security of data held electronically by way of appropriate use of IT security methods and systems (e.g., password protection and data encryption where necessary). Euromed will also ensure that paper records are held securely. This includes ensuring documents containing personal and sensitive information is only available to those with legitimate need to access such data.

The company will take reasonable steps to ensure that the data it holds and processes is done fairly and that excessive information is not requested or stored.

The company will periodically take reasonable steps to ensure that the data it holds is up-to-date by reviewing the information on employee, client and supplier records. It will be the responsibility of employees, clients and suppliers, to provide updated information in a timely manner following any such request to do so. This review process is not generally considered necessary for the purpose of patient records.

Data will be stored for a time considered reasonable based on the nature of information held. Due to the variety of records held it is not appropriate to apply a blanket timeframe. The company therefore uses the guidelines published by the NHS Executive in respect of patient records.

Data held in relation to staff will be held in accordance with guidance set by HMRC for the purposes of accounting, tax and NI. This period will be 7 years from the date of last entry onto an employee record.

For all other records failing outside of the above, the company will maintain data for a minimum of 3 years from date of last entry and a maximum of 10 years from date of last entry. After this time, records will be destroyed in accordance with the procedures outlined below.

Data restrictions

Data owners have the right to restrict the use of the personal data, for example upon request data held will not be used for the purposes of marketing correspondence unless requested to do so.

Euromed will not contact the data owner without permission.

If the data owner requests personal data to be withheld in medical confidence this restriction can be superseded by the medical personnel in attendance if it related to the patients well being only when shared with medical professionals as part of the patient care pathway.

Data Objections

An individual or business can register objections to their data being held, in doing so data should not be processed or stored and must be permanently deleted. With the exception of patient information relating to treatment of the individual if it affects the wellbeing of the patient in question.

Destruction of Data and Records

Electronically stored - all data will be electronically deleted from any

active and archived records

Paper records - all data will either be shredded on site or securely destroyed by the company engaged by

Euromed to handle confidential waste.

Subject Access Request

A subject access request (SAR) is simply a written request made by or on behalf of an individual for the information which he or she is entitled to ask for under section 7 of the Data Protection Act 1998 (DPA). The request does not have to be in any particular form

Individuals have the right to access their personal data.

This is commonly referred to as subject access.

Individuals can make a subject access request verbally or in writing.

Data Loss and Breach

The company will take reasonable measures to ensure that all data is maintained securely at all times, but accepts there may be occasions where data is lost or breached through human error or malicious attacks on stored data.

Any loss or breach of data by any means must be notified to the Data Controller within 24 hours of discovering such loss/breach.

The Data Controller will be responsible for co-ordinating the company response and management of such a loss/breach. This will included notifying the ICO where necessary.

All employees/contractors have a duty to report the loss of company data to the Data Controller within 24 hours. Failure to do so may result in disciplinary action and potential legal action.

The inappropriate use of company data by an employee/contractor will result in disciplinary proceedings and may also constitute the need for criminal proceedings and action by a professional/regulatory body. The company has a duty to report any illegal activities by any employee/contractor.

Any data subject affected by the loss or breach of data will be notified in writing within 48 hours. This notification will outline the nature of any such incident as well as the actions taken by the company to minimise the loss/breach and to rectify any damaged incurred by such a loss/breach.

The company will take all reasonable steps to attempt recovery of any data loss/breach or to minimise the damage caused by such loss/breach.

The company will carry out an internal investigation and review of procedures in the event of any data loss/breach.

Access to data by employees, clients and service users

The company acknowledges that from time-to-time it may receive subject access requests from employees, clients and services users and that it has a legal duty to respond to these requests within 28 working days.

It will be the responsibility of the Data Controller/Data Protection Lead to manage any subject access requests. However, all staff must ensure that any such requests are passed to the Data Controller/Data Protection Lead in a timely manner and that such requests can also be made verbally.

The company will not charge a fee for handling standard subject access requests or for medical subject access requests. Notification will be made in the initial response by the Data Controller/Data Protection Lead following a subject access request.

Where necessary, the Data Controller/Data Protection Lead will take reasonable steps to verify the identity of any person making a subject access request.

The provision of data held by Euromed following a subject access request will normally be made in permanent form through printed records. These will then be sent to the individual making the subject access request by recorded mail delivery and marked as confidential and for the addressee only.

The Data Controller/Data Protection Lead will follow the guidance issued by the ICO at the time of any such subject access requests. This will include consideration of any exemptions that apply to the non-disclosure of data following a subject access request (see 4.4 below).

Policy Awareness

The company will ensure awareness of this policy through:

Electronic publication of this policy to staff

Electronic updates to staff (email, newsletters and other electronic means)

Staff induction/training (where necessary)

Reference to the ICO on the company website

Policy Updates

This policy will be reviewed on a biennial basis, unless there are changes that occur in law during this time which have significant influence on the policy. In such cases it will be reviewed accordingly.

Any amendments and changes to policy will be communicated to staff as necessary.

This policy will be reviewed on a biennial basis, unless there are changes that occur in law during this time which have significant influence on the policy. In such cases it will be reviewed accordingly.

Any amendments and changes to policy will be communicated to staff as necessary.

Appendix 1 - Caldicott Principles - Patient Confidentiality

Objectives

All Euromed staff who are engaged in processing personal data in executing their duties should apply the six general principles of good practice in handling patient-identifiable information as set out by the Caldicott Principles.

Principles

Access to patient-identifiable information should be restricted to those staff who have a justifiable need to know in order to carry out their jobs effectively. These principles are:

Principle 1 - Justify the purpose(s) Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2 - Don't use patient-identifiable information unless it is absolutely necessary Patient-identifiable information items should not be used unless there is no alternative.

Principle 3 - Use the minimum necessary patient-identifiable information Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.

Principle 4 - Access to patient-identifiable information should be on a strict need-to-know basis Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.

Principle 5 - Everyone should be aware of their responsibilities Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Understand and comply with the law Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

Compliance

It is imperative that all staff members adhere to these principals in the course of their duties. Any staff member who fails to do so may be subjected to disciplinary procedures. Any member of staff who requires clarification of these principles should, in the first instance, contact their line manager. Otherwise they should contact another member of the management team or the company Data Controller or Data Protection Lead.

Source: Protecting And Using Patient Information, A Manual for Caldicott Guardians