Criticare UK Ambulance Service

Independent Service Provider

Policy Document

Data Protection v3.2

Written: February 2013

Author: David Seymour, Director of Operations

Approved: Board of Directors

1. Statement of Intent

Criticare UK Ambulance Service (the Company) intends to fulfil all its obligations under the Data Protection Act 1998 (the Act). The Company will ensure that the Information Commissioner is notified of all relevant processing and will conduct a periodic review and update of the register entries to ensure that they remain up to date. It is the aim of the Company that all appropriate staff are properly trained, fully informed of their obligations under the Act and are aware of their personal liabilities.

Criticare UK Ambulance Service as a data controller is required to notify the Information Commissioner under the Data Protection Act 1998. The Company's registration number is:

Z1689891 (Expires 16/03/2013)

The Company will use the exemptions available to it to gather the necessary data to provide its patient care services to the public. The Company will share information with other agencies, where it is legal to so do, if this enhances its ability to provide services that affect a person's health or where the Company needs the support of another agency to secure that patient care for an individual. Any sharing arrangements will be based upon formal protocols and will be in accordance with the eight data protection principles.

The Company will secure and maintain such data as is necessary to assist in the protection of the health and safety of its staff while continuing to comply with obligations to patients and others under the Act.

Individuals whose information is held and processed by the Company can be assured that it will treat their personal data with all due care. Any employee deliberately acting outside of their authority will be subject to disciplinary procedures, up to and including dismissal where appropriate, and to possible legal action by the Company. Any action to initiate legal proceedings must be approved by the Board of Directors.

Where the Company is not the data controller but rather the data processor it will abide by any written agreement between it and the data controller on data protection policy. This means where we process data collected by others and we are providing processing or some related service, for example Patient Transport Services for a hospital trust, then the Company will ensure the hospital's data protection rules are implemented as has been agreed in writing.

This policy document applies only to information covered by the Data Protection Act 1998 and will be updated/amended as necessary according to the laws of England and Wales.

2. Fair Obtaining/Processing

The Company will, as far as is practicable, ensure that all individuals whose details it holds are aware of the way in which that information will be held, used and disclosed. Individuals will, where possible and practicable, be informed of the likely recipients of the information – whether the recipients are internal or external to the Company. Processing within the Company will be both fair and lawful and individuals will not be misled as to the uses to which the Company will put the information given. If a person feels they have been deceived or misled as to the reason for which their information was collected, they should use the complaint procedure detailed at the end of this document.

Forms requiring personal information will (if possible) contain a 'fair obtaining statement' giving details of the likely uses of the information and where information is collected in person or by telephone, the employee asking for the details will tell the individual how those details will be used. People are free to ask the person collecting the information why they want the details and what they will be used for.

Example of 'fair obtaining statement':

> The information you have provided will only be held for the purposes of providing patient care, now or in the future, to you or to someone else on whose behalf you may be acting.

Where the Company is using an exemption under the Act to obtain personal information that, in all of the circumstances, makes a fair obtaining statement impractical then no such statement will be made. Examples of this would be where:

- A call taker needs to focus on collecting data that is time critical in order to protect the vital interests of the, or an, individual
- Medical personnel collecting information from or about a patient and the care of that patient must take priority in the patient's own vital interests

If a person's details are going to be used for 'auto-decision' processing (where a computer decides something based on a score or other information) the person will be entitled to be told about how the system works and whether the decision can be challenged.

If a person's details are to be processed for a purpose that does not appear on the Company's entry (e.g. some new processing not previously notified) the individual will be given the information that would be necessary to make the processing fair and lawful. The Company will undertake to make a formal notification to the Information Commissioner as soon as possible in these circumstances.

Any individual whose personal data (including photographs) are to be included on the Company's web site will be asked to give their explicit consent. At the time of data collection, it will be made clear to individuals that details published on the Company's web site are viewable by anyone, anywhere in the world, who has access to the Internet.

3. Data Uses and Processes

The Company will not use or process personal information in any way that contravenes its notified purposes or in any way that would constitute a breach of data protection law. Any new purposes introduced will, where appropriate, be notified to the individual and – if required by the law – their consent will be sought.

All staff using personal data within the Company will be told the limits of their authority to use and disclose such information through their managers and supervisors, the induction process and regular update bulletins.

4. Data Quality and Integrity

The Company will not collect data from individuals where that information is excessive or irrelevant in relation to the notified purpose(s). Details collected will be adequate for the purpose and no more. Information collected which becomes (over time or by virtue of changed purposes) irrelevant or excessive will be deleted. All of the Company's departments will create working procedures, with standards that can be monitored, for managing data collection and updating of records such that accuracy, relevance, consistency with purpose and quality are assured.

Information will only be held for as long as is necessary for the notified purposes – after which the details will normally be deleted. Where details of individuals are stored for long-term archive or historical reasons and where it is necessary to retain the personal detail within the records it will always be done within the requirements of the legislation. Appropriate closure periods will also

be set, to protect data subjects. In some cases personal details will be removed from the record so that individuals cannot be identified.

The Company will ensure, as far as is practicable, that the information held is accurate and up to date. It is the intention of the Company to check wherever possible the details given. Information received from third parties (i.e. neither the individual concerned nor the Company) will carry a comment indicating the source, where practicable.

Where a person informs the Company of a change of their own circumstances, such as home address or non-contentious data, their record(s) will be updated as soon as possible. Where the individual requests that information be changed and it is not possible to update it immediately, or where the new information needs to be checked for its accuracy or validity, a comment will be placed on the disputed record indicating the nature of the problem. If the system does not allow the individual record to be marked in this way, departments will ensure that a manual record is made of the request and that it is processed within a reasonable time-scale.

Every effort will be made to reach an amicable agreement on any disputed data. Where this is not possible, the Company will implement its complaints procedure.

An internal investigation will be implemented if there is any alleged improper misuse of personal data by staff and appropriate action will be taken.

5. Technical and Organisational Security

The Company has implemented appropriate security measures as required under the Data Protection Act 1998. In particular, unauthorised staff and other individuals are prevented from gaining access to personal information. Appropriate physical security is in place.

Computer systems are installed with user-profile type password controls to ensure data is only accessed by authorised users, and where necessary, audit and access trails to establish that each user is fully authorised. In addition employees are fully informed about overall security procedures and the importance of their role within those procedures. Manual filing systems are held securely and are accessed on a need-to-know basis only.

Security arrangements are reviewed regularly. All reported breaches of security are investigated and where necessary, further or alternative measures are introduced.

All staff are informed and regularly reminded about the limits of their authority on disclosing information both inside and outside the Company. Where details need to be passed outside the Company, it will in general be done with the person's consent except where this is not possible or where it is required by law (such as crime prevention/detection, prevention of injuries etc.) or where it is in the person's vital interests. Any unauthorised disclosure will be dealt with under the Company's disciplinary procedures.

Redundant personal data will be destroyed using the Company's procedures for disposal of confidential waste. In general, paper waste is shredded and magnetic media (disks, tapes, etc.) are either electronically wiped or physically destroyed beyond recovery.

6. Subject Access/Subject Information Requests

The Data Protection Act gives individuals the right to see information held about them and the same Act places a duty on the Company to make that information available. Any person whose personal details are held/processed by the Company has a right to receive a copy of his or her own information. There are a few exceptions to this rule (examples being data held for child protection, crime detection/prevention purposes or where the information is likely to cause serious harm to the physical and/or mental health of the patient or other individual) but most individuals will be able to have a copy of the data held about them.

Where any information relates to an identifiable third party, other than the data subject, consent must be gained from that third party, before any information relating to them can be released.

The Company has the right to make a charge for such requests for computer based data and data held on paper or other media. An appropriate charge will be levied for this in line with the prevailing guidance at that time.

The Company will reply to subject access requests as quickly as possible and in all cases within the 40 days allowed by the Act. Repeat requests will be fulfilled unless the period between is deemed unreasonable, such as a second request received so soon after the first that it would be unlikely for the details to have changed. A subject access/information request should be submitted on

the appropriate forms wherever possible - this will ensure that the Company has the required information to be able to conduct a data search and to fulfil the request. In some cases, especially with requests not submitted on the correct form, further information may be required from the requester which may delay the start of the 40 day maximum time limit.

7. Further Information, Enquiries and Complaints

The Board of Directors should be contacted to raise any issues regarding this policy document. The responsibility for dealing with any internal or external enquiries rests with the Board of Directors. Where possible, requests for detailed information should be in writing.

Any complaints must be written, dated and must include details of the complainant as well as a detailed account of the nature of the problem. The Company will attempt to complete internal investigations within twenty days and in every case the person will receive an acknowledgement as soon as possible after the complaint is received.

Complaints should be sent to:

Director of Discipline and Professional Standards
Criticare UK Ambulance Service
Elvaston
Pooks Green
Marchwood
Hampshire
SO40 4WP

5. Review

The Board of Directors will ensure that this policy is reviewed on an annual basis.

Review date: March 2013