Fair Processing (Privacy) Notice

Introduction

This guide explains what information is collected about you, why it is collected and the ways it is used. First Care Ambulance Ltd recognises how important it is that you are fully aware of the information we collect and hold about you as well as how we share that information.

To ensure that your information is kept confidential and that our data is kept safe and secure, all our staff are given training in data protection and information governance before they start work with us. Current staff must also undertake regular refresher training courses tailored to their individual roles.

Who we are and what we do

- First Care Ambulance Ltd
- Unit 16/17 Kestrel Way
  Kestrel Business Park
  Sowton Exeter Devon EX2 7JS
- 01392 438522
- office@firstcareambulance.net
- www.firstcareambulance.net

FCA provides non-emergency patient transport services to Devon and the South West.

Access to your information

Our staff will only have access to information that is necessary for them to complete the business activity they are involved in. This is reflected in Caldicott Principles that access to your information should be on a need to know basis only. Staff access of confidential information is monitored to ensure your confidentiality is maintained.

Types of Personal Information we handle

We process personal information to enable us to support the provision of healthcare services to patients, maintain our own accounts and records, promote our service, and to support and manage our employees. We also process personal information about healthcare workers that deliver services throughout First Care Ambulance.

- Personal details such as your name, address, telephone number(s), and date of birth
- Family details such as next of kin details
- Education and training records of our staff

- Employment details, for example for those that work directly for us or are commissioned by us to provide a service on our behalf
- Visual images, personal appearance and behaviour, for example if CCTV images are used as part of building security.
- Details held in the patient's records required for the safe planning and transportation of our service users
- Responses to surveys, where individuals have responded to surveys about healthcare, data security issues
- Details of each contact that we have had with you, including home visits and telephone consultations
- Records of your health and wellbeing, including reports from other health and care providers
- Relevant information from people who care for you, including other health and care providers, carers and relatives

This information is referred to as Person Confidential Data and we are mandated to ensure that it is treated in confidence and with respect, using the Caldicott Principles as our basis for managing your information.

Types of Sensitive Information we handle:

We may also process sensitive classes of information that may include:

- Racial and ethnic origin
- Offences (including alleged offences), criminal proceedings, outcomes and sentences
- Trade union membership
- Religious or similar beliefs
- Employment tribunal applications, complaints, accidents and incident details

This information will generally relate to our staff. In terms of patient information, this may include:

- Physical or Mental health details

What Information First Care Ambulance collects about you and Why.

We only collect and use your information for the lawful purposes of administering the business of NHS England. These purposes include:

- Planning and booking patient ambulance journeys
- Accounting and Auditing
- Accounts and records
- Health administration and services

How we keep your records confidential

Everyone working for the NHS is subject to the Common Law Duty of Confidence and governed by the Data Protection Act. Information provided in confidence will only be used for the purposes advised and consented to by the patient, unless there are other circumstances covered by the law.

Under the NHS Confidentiality Code of Conduct, all our staff are also required to protect your information, inform you of how your information will be used, and allow you to decide if and how your information can be shared. NHS England have produced some informative tools on how public information is shared.

How your records are used

Your records are used to guide healthcare professionals in the care you receive:

- Your records help inform the decisions that we make about your care;
- Your records ensure that your treatment is safe and effective, including any advice that may be provided as part of your care;
- Your records help us to work effectively with other organisations who may also be involved in your care;
- Your records help us to thoroughly investigate any feedback or concerns you may have about contact with our services;
- Your records may also be available if you see another doctor, or are referred to a specialist or another part of the NHS or health care system for the purposes of direct care;
- Your records help us to investigate complaints, legal claims and untoward events;
- Your records help us to prepare statistics on NHS performance;
- Your records assist with health research and development;
- Your records help us to teach, train and monitor staff and their work (including providing staff and clinicians with anonymous feedback from patient surveys) to audit and improve our services and ensure they meet your needs;
- Your records help us to conduct clinical audit to ensure we are providing a safe, high quality service;
- Your records help us to support the provision of care by other healthcare professionals;

Using information for purposes other than direct healthcare

Healthcare organisations, such as your GP or the hospital that you visit, hold information about you in order to support the treatment that is provided. There are measures outlined in law which protect the information that is held by these organisations. These measures ensure that information is only shared appropriately and in line with your wishes.

Organisations will use this information to support you with any treatment or contact that you may have, which is known as for direct care purposes. It helps them provide the most appropriate care for you as an individual and they may share information with other health professionals to ensure that they can make informed decisions. Where this information is

shared, your confidentiality and privacy will be protected. To make sure this takes place, there are clear rules in our own procedures as well as national legislation.

As well as this information supporting your care, reports are produced which contain information to help plan future healthcare services, which is termed as for non-direct care purposes. This information is used to identify areas where our services need to expand, to improve & to change, in order to support our population fully and also to support the flow of funding from one NHS organisation to another. There are clear processes in place to say how this information can be used and what safeguards must be in place to protect patients. The ways in which information should be made anonymous are governed by the Department of Health.

FCA uses three different types of information:

1) **Person Identifiable Information (PII) confidential data** – information which on its own or with other information can identify you.
2) **Anonymised data** – where unique identifiers such as your name and full address have been removed so the information is no longer 'person identifiable'.
3) **Pseudonymised data** – where personal information about you is replaced with a code. We retain the key to the code so would know which person this information related to but a third party who we shared this data with would not. This is often used for example, when information is needed for research purposes.

Where possible, we ensure your information is anonymised or pseudonymised (especially when using information for purposes other than for direct patient care).

Team members that carry this out have all been approved to carry out this work by our Caldicott Guardians.

For all other uses of your personal information we will either directly ask for your consent or, use anonymised data that does not identify you. For example, it may be that we use anonymised and/or pseudonymised data for:

- Processing information – changing information so it can be used for secondary purposes
- Research
- Local and national benchmarking
- Audits - including local clinical audit to provide quality assurance of the care received by our service users
- Service management
- Commissioning and commissioners reports (e.g. to CCGs)
- Contract monitoring
- Capacity and demand planning
- Reporting, including public health alerts, performance and board reports
- Teaching and training
- Sharing best practice/serious case reviews/incident management of adverse events
- Staff and patient surveys

- Personal development/review (particularly for clinicians)
- Subject access requests
- Risk stratification

Third parties we share information with

There are circumstances where we need to share information without your consent. For example, when the health and safety of others (including members of staff) is at risk, to ensure we provide you with the correct care, to protect public health or when the law requires information to be passed on. Or for the prevention or investigation of serious crime, under a court order, when sharing is in the public interest, where there are safeguarding concerns for vulnerable people.

Information may be withheld if it is believed it may cause serious harm or distress to you or to another person.

Sometimes it is necessary for us to share information with another organisation. For example, you may be receiving care from social services and we may need to share information about you so we can all work together for your benefit.

We will only ever use or pass on information about you if others involved in your care have a genuine need for it. Anyone who receives information from us is also under a legal duty to keep it confidential and secure.

We may also share your information with organisations such as:

- NHS Trusts
- Community/district nurses
- The ambulance or other emergency services
- Other General Practitioners
- Child and adult safeguarding services e.g. MASH
- Social Services
- Local Authorities
- NHS 111
- Care Quality Commission and other regulated auditors e.g. the ICO
- Public Health England
- HSCIC

Your rights

You have the right to confidentiality under the Data Protection Act 1998 (DPA), the Human Rights Act 1998 (HRA), the Health and Social Care Act 2012 (HSCA) as well as the common-law duty of confidentiality. The Equality Act 2010 may also apply in some circumstances.

You have the right to know what information we hold about you, what we use it for and if the information is to be shared, who it will be shared with.

You have the right to:

- Apply for access to your records (SAR);
- Obtain a copy of your record in a permanent form; and
- Have the information provided to you in a way you can understand and explained where necessary, such as when abbreviations are used.

Where you agree, the access right may be met by enabling you to view your record, without obtaining a copy.

Under normal circumstances we will not transfer your information outside of the European Economic Area, however there may be occasions where you require this information to be sent. In these instances, we will ask for and record your consent to do so and will take reasonable steps to ensure the safety of the information that is sent.

Your right to withdraw consent for us to share your personal information

At any time, you have the right to refuse/withdraw consent to information sharing. The possible consequences will be fully explained to you (this could include delays in receiving care).

How can you get access to your own health records?

> The Data Protection Act 1998 gives you the right to see or have a copy of your health records. You do not need to give a reason, but you may be charged a fee.
>
> The General Data Protection Regulations (May 2018), Chapter 3 Section 2 gives you the right to

How do we keep your records confidential and secure?

The sharing of your information is strictly controlled. We will not pass on information about you to third parties without your permission unless there are exceptional circumstances, for example, where we are required to by law.

In all cases, where personal information is shared, either with or without your consent, a record will be kept. We also adhere to the revised Caldicott Principles to make sure information is accessed and held securely and appropriately.

Our secure networks, internal and external IT safeguards and audits all ensure we protect your right to privacy and confidentiality. We only keep your records as long as we need to and are required to by law / national codes (for example, the NHS Records Management Code of Practice) after which they are securely destroyed.

How you can access your records

The Data Protection Act 1998 allows you to find out what information about you is held on computer and in certain paper records. This is known as a 'right of subject access'. If you would like to see your records you can make a written request to us. You are entitled to receive a copy of your records and do not have to give a reason for the request, however, there may be a charge, to cover the administrative costs.

Consent will be required when requesting information relating to someone else. To make such a request, please refer to the leaflet 'How to access information'.

Leaflets

To help you to understand what information we collect and how we use it please see our leaflet(s) and website for further information, alternatively one of our staff will be happy to discuss this further with you.

- Your information: your rights, our responsibility
- How to access information

These are available on our website in both standard text and easy read versions:

Queries, comments, concerns or objections

Should you have any queries or objections in relation to how we use your information or if you require this guide in an alternative format such as large print (or another language) please contact our Information Governance Lead via email office@firstcareambulance.net

Information Governance Lead
First Care Ambulance Ltd
Unit 16/17 Kestrel Way
Kestrel Business Park
Sowton
Exeter
Devon
EX27JS

You have the right at any time to request your information is not used in this way and to have your objections heard. We will comply with your request where we are able to do so in accordance with the law. We will discuss with you how this may affect our ability to provide care or treatment and any alternatives available to you.

To provide a safe, professional and efficient service, we need to keep information on record. Your personal details will be handled with sensitivity and confidentiality. We would encourage all patients to make sure their details are correct and kept up to date, especially if you change your name, address or telephone number. If you think any information we hold about you is not accurate, please let us know.

You have the right to view your records and request mistakes are corrected, but not to change the content as this may be clinically unsafe. If you are not happy with an opinion or comment, we will add your comments to your record.

We use your information in accordance with legislation such as the Data Protection Act 1998, the NHS Care Record Guarantee and the NHS Confidentiality Code of Conduct, all of which can be accessed online or posted on request. If you feel we are not following these commitments in any way, please tell us and we will fully investigate your concerns.

For more information on how your personal information is used please see our website www.firstcareambulance.net

Appendix A - Our obligations under the General Data Protection Regulations 2018; the Data Protection Act 1998 & the Human Rights Act 1998

General Data Protection Regulations 2018

Data Protection Act 1998

The data protection act 1998 says:
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

This is the first data protection principle. In practice, it means that you **must**:
• have legitimate grounds for collecting and using the personal data;
• not use the data in ways that have unjustified adverse effects on the individuals concerned;
• be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
• handle people's personal data only in ways they would reasonably expect; and
• make sure you do not do anything unlawful with the data.

Fairness generally requires you to be transparent – clear and open with individuals about how their information will be used. Transparency is always important, but especially so in situations where individuals have a choice about whether they wish to enter into a relationship with us.

Once it has been established that a data controller does have the "lawful" power to share personal data it would then need to satisfy a Schedule 2 condition for processing and where sensitive personal data is involved, a Schedule 3 condition. It should be remembered though that even where a condition or conditions for processing can be met this will not on its own ensure that the processing is fair or lawful.

These issues need to be considered separately.

It is also worth briefly looking at the issue of "consent" To the ICO "consent" means just that. For example someone is asked if their information can be used in a certain way. If they agree release of information can proceed, but if they refuse their consent, then in the view of the ICO, their wishes should be respected and the information should not be used.

In addition it needs to be remembered that in data protection terms "consent" is but one condition that could be relied on to process personal and sensitive personal data. There are several other conditions that it may be possible to rely on depending on the purpose of the processing (and which are set out in Schedule 2 and in Schedule 3).

In terms of meeting a Schedule 2 condition there are two that could be relied on these are:
5. The processing is necessary –
(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

or
6. – (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Meeting a Schedule 3 condition is more difficult (and which is the way it should be). However in these circumstances the ICO considers that a condition provided for in SI 417 (2000) [1]could be met, namely:
The processing –
(a) is in the substantial public interest;
(b) is necessary for the discharge of any function which is designed for the provision of confidential counselling, advice, support or any other service; and
(c) is carried out without the explicit consent of the data subject because the processing –
(iii) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the provision of that counselling, advice, support or other service.

The ICO stresses that where these conditions are being relied upon that there is the provision of fair processing information to the individuals involved, with more information being required where the data sharing is more extensive. Privacy notices should make it clear to individuals about how their information is being used and where they can find out more about the processing and/or object to the processing (s10 of the DPA).

As the conditions above require that the sharing is either in the substantial public interest or is for confidential counselling purposes added to the fact that public authorities must not act in any way that is incompatible with the Human Rights Act we will seek the explicit informed consent of the patient or individual. It is also important to ensure that the other Data Protection principles are complied with e.g. the information shared needs to be relevant and not excessive, it must be accurate and kept up to date, not kept for longer than necessary and kept secure.

If individuals know at the outset what we propose to use their information for, they will be able to make an informed decision about whether to:
(a)enter into a relationship with us, or perhaps to try to renegotiate the terms of the relationship;
(b) consent or dissent to the use of their information.
If anyone is deceived or misled when the information is obtained, then this is likely to be unfair and will be a breach of the DPA.

The Data Protection Act says that information should be treated as being obtained fairly if it is provided by a person who is legally authorised, or required, to provide it. The Data Protection Act does not define 'lawfully'. However, "lawful" refers to statute and to common law, whether criminal or civil. An unlawful act may be committed by a public or private-sector organisation.

If processing personal data involves committing a criminal offence, the processing will obviously be unlawful. However, processing may also be unlawful if it results in:

[1] Statutory Instrument 2000 No. 417 The Data Protection (Processing of Sensitive Personal Data) Order 2000

• a breach of a duty of confidence. Such a duty may be stated, or it may be implied by the content of the information or because it was collected in circumstances where confidentiality is expected – medical information, for example;
• the organisation exceeding its legal powers or exercising those powers improperly;
• a breach of industry-specific legislation or regulations;
• a breach of the Human Rights Act 1998. The Act implements the European Convention on Human Rights which, among other things, gives individuals the right to respect for private and family life, home and correspondence.
For more information please see the Information Commissioners website:
http://ico.org.uk/

Human Rights Act 1998

S6 Human Rights Act 1998 (HRA) makes it unlawful for a public authority to act in a way that is incompatible with a person's rights under the European Convention on Human Rights. Another way of putting this is to say that all public authorities must comply with the Human Rights Act and their decisions can be challenged in court.

Therefore staff must be aware of convention rights and must understand the 'positive obligations' of the Act.

The NHS Constitution also outlines the rights of patients and what they can expect from the NHS
http://www.nhs.uk/choiceintheNHS/Rightsandpledges/NHSConstitution/Pages/Overview.aspx

For further information please see the' Your rights' website
http://www.yourrights.org.