Falck	Always check on-line for validity. **Privacy Commitment to Patients**				Level: **Support Processes** Approved by: **claire.ward 16.10.2018**
Document users: **FalckUK-AMB**	Editor: **claire.ward**	Responsible: **HeadHSEQ**	Document number: **46422**	Version: **1**	

1) Introduction

1.1 As a provider of first response and patient transport services, Falck UK Ambulance Service (Falck UK) acts as data controller and processor for certain personal data about patients.

1.2 Falck, as a data controller and processor, has a duty to protect the personal data we process about our patients. If you are interested you can read more about the framework for controlling and processing personal data in our General Data Protection Regulation (GDPR) Policy, and Falck Group's Personal *Data Protection Policy* and *Information Security Policy*. As part of this framework we have a suite of information governance, information technology (IT), and records management policies, and have accreditation for ISO 27001: Information Security.

1.3 This privacy commitment describes our processes for collecting, holding, using and transferring of the personal data of our patients. It sits within our information governance, information technology and records management framework of policies and processes (information governance policies) and is overseen by the Health Safety Environment and Quality (HSEQ) Team, with support from our IT services provider.

1.4 This commitment defines, to our patients, our responsibility for protecting their personal data in accordance with the European Union (EU) General Data Protection Regulation (GDPR), effective from May 2018. Consequently, it is worded in terms that express these responsibilities.

1.5 Personal information, held about you, our patients, will not be shared, sold or disclosed in any manner other than as described in this privacy commitment.

2) Responsibilities

2.1 The Data Protection Officer (DPO) for Falck Group is: Birgitte Poulson, who may be contacted at: DPO@falck.com or +45 30 50 18 46.

2.2 Responsibility for GDPR compliance in the United Kingdom is delegated to the Director of Quality & Operations; who has responsibility for the administration and implementation of Falck UK's GDPR Policy.

2.3 These executive responsibilities are delegated to the Head of HSEQ. Therefore this commitment, which was prepared by Falck Group, was modified for Falck UK by the Head of HSEQ. Future reviews will also be conducted by the Head of HSEQ.

2.4 All directors and managers are responsible for ensuring that their teams are aware of their responsibilities in relation to the collection, storage and handing of the personal data of patients. They must ensure that patients are aware of the reasons why we may collect some

items of personal data and have consented to its use for the purposes we have described to them. These responsibilities are outlined within our information governance policies.

2.5 Relevant directors sign, data sharing agreements for the systems we jointly use with Falck Group, on behalf of Falck UK. This responsibility is defined by the personal data that is used within their directorate.

3) Procedures

3.1. Statement to patients

3.1.1 We collect, hold and process personal information only to enable us to provide suitable transport for you to and from appointments for admission and discharge from hospital. To help us to investigate, analyse, and learn from problems that occur we also record information about complaints, concerns and incidents that occur in the delivery of these services.

3.1.2 Whilst you are not obliged to provide personal information to us. If you do not provide us with information essential to our ability to provide a safe service to you we retain the right to refuse to transport you.

3.1.3 You have, within the limitations of the legislation, among other things: the right to: access your personal data; rectify incorrect information; request deletion or limitation of information; data portability; and object to the processing of personal data. However, you must be mindful that we have the right to refuse if not having access to the data may significantly impair our ability to run our services safely and efficiently.

3.1.4 All patients may raise concerns about the treatment of personal data and instances when the security of their personal data may have been breached. All requests for data access are handled in accordance with our information governance policy and complaints are managed in accordance with our registrations policy.

3.1.5 You also have a right to raise a concern with the Information Commissioner's Office, as the supervisory authority [
https://ico.org.uk/].

3.2. Collection of personal data

3.2.1 Personal data, which is held about you may include:

- Name, address, e-mail address and telephone number
- Health care information
- Information held to make a safeguarding referral

3.2.2 All personal data we hold is held securely for periods defined by the NHS and is only used to enable us to deliver our services in accordance with our values: efficient, reliable, competent, helpful, accessible and fast.

3.2.3 It is essential that appropriate changes to this data are recorded and we may therefore ask you to confirm the details of the information we hold.

3.3. Automated, individual decision making

3.3.1 Personal data is not used for automated, individual decision making or profiling.

3.4. The legal basis for processing the personal information

3.4.1 The legal basis for processing of general and sensitive personal data as outlined above is the delivery of first response and patient transport services with the consent of patients (cf. article 6(1)(b&b))

3.4.2 The personal information collected about you or employment purposes supports our contracts with you as our patients.

3.4.3 Please refer to the Checklist - Legal basis for processing personal data in our GDPR Policy.

3.5. Disclosure of personal information

3.5.1 Personal information collected by Falck UK may be disclosed to and shared with the following recipients:

- Falck Group: The Falck Group's parent company
- Commissioning clinical commissioning groups and ambulance trusts
- Hospital trusts, hospices, care homes and agencies who care for our patients
- Local authority staff, in relation to safeguarding
- Police and other emergency services
- Carers, next of kin and other necessary individuals in the event that a patient is not able to speak for themselves
- External and internal auditors

3.6. Special category data

3.6.1 We will pay particular regard to the security of personal data defined as special category data under GDPR, which may include:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation

3.7. Transfer of personal information to data processors

3.7.1 We transfer your personal data to certain suppliers, e.g. IT suppliers, who process the information on behalf of Falck.

3.7.2 Transfer of personal data to recipients in countries outside European Union (EU)/European Economic Area (EEA).

3.7.3 We transfer your data to recipients in countries outside EU/EEA as we use an external supplier to host/store the above mentioned personal information. The basis for the international transfer is EU's "Standard Contractual Clauses" for transfers from data controllers to data processors in countries without an adequate level of protection outside EU/EEA.

3.7.4 The standard agreement is available in different languages via this link: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1401799946706&uri=CELEX:32010D0087.

3.7.5 Please refer to the Checklist - International transfers of personal data in our GDPR Policy.

3.7.6 Further information about data providers and transfers to recipients outside the EU/EEA can be obtained from the IT department (it.servicedesk@falck.dk)

3.8. Retention periods

3.8.1 We retain your personal data as long as necessary, in accordance with NHS defined retention periods (https://digital.nhs.uk/records-management-code-of-practice-for-health-and-social-care-2016) in order to fulfill the above stated purposes. It is acknowledged that the code of practice and related retention period schedule is currently under review and our practices will be amended to reflect the new code of practice once published.

3.9. Contact details

3.9.1 If you have any questions or comments with respect to the processing of your personal data or you wish to exercise your rights under applicable legislation, please contact Lezli Feeney, Head of Health Safety Environment and Quality [lezli.feeney@medicalservicesuk.com]. Support in responding to you request will be provided by the Director of Human Resources and our IT services provider. You may also our global group data protection officer by emailing to dpo@falck.com or writing to:

Falck [Danmark] A/S

Polititorvet 1

1780 København V

Date: 18 April 2018

4) Related policies/procedures

Information governance policy
Data protection policy

Information security policy
Clinical records policy
Records management policy
Misuse of social media policy
Whistleblowing policy

5) References

EU GDPR Portal (2018) *Site overview* [online] **https://www.eugdpr.org/**
NHS Digital (2016) *records management code of practice* [online] **https://digital.nhs.uk/records-management-code-of-practice-for-health-and-social-care-2016**

6) Appendices

19112 General Data Protection Regulation (GDPR) Policy
19125 Information Governance Policy
20535 Whistleblowing UK Policy
32203 Information Security Policy
37611 Misuse of Social Media
38092 Records Management Policy including Clinical Records

Version history

Version	Approval	Revision information
1	24.05.2018	
1.0	16.10.2018	