Carfax Health Enterprise CIC

Data Security and Protection Policy

Introduction

Everyone has rights with regard to how their personal information is handled. We collect store and process personal data about our staff and patients and recognise the need to treat it in an appropriate and lawful manner.

The types of information that we may be required to handle include details of current, past and prospective employees, suppliers and patients. The information may be electronic or hardcopy and is subject to Data Protection legislation, the EU General Data Protection Regulations, UK Data Protection Act 2018 and Access to Health Records Act 1990. The legislation imposes restrictions on how we use that information. In addition to Data Protection legislation all information is held under legal and ethical obligations of confidentiality. Information in confidence should not be used or disclosed in a form that might identify an individual unless the individual has consented or there is an overriding legal reason to do so.

Principles

Anyone processing data must comply with the principles of good practice. These state that data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specific, explicit and legitimate purposes and not further processed in a manner that is not compatible with those purposes.
- Adequate, relevant and limited to what is necessary for the purpose.
- Accurate and up to date.
- Not kept longer than necessary.
- Processed in a manner that ensures appropriate security.

Carfax Health Enterprise will maintain records of its processing activities, recording:

- The types of data collected.
- How data is stored.
- The purposes it is used for.
- Disclosures of data to other agencies.

It will also have records of staff training on data protection and audits done to ensure that it is complying with legislative requirements, such as the Data Security & Protection Toolkit.

Processing

Legislation ensures that data processing is done fairly and without adversely affecting the rights of the data subject. The data controller is Sarah Smith, the Data Protection Officer.

The data subject should also be able to access detail on:

- The lawful basis for which data is being processed.
- Who data is being disclosed or transferred to.
- The retention period for their data.
- Their rights to raise concerns with the Information Commissioners Office.

For personal data to be processed lawfully certain conditions have to be met. For the provision of care to patients, the general lawful basis is the 'exercise of official authority' and the 'provision of health and social care services and treatment'. Detailed guidance on lawful basis has been published by the Information Governance Alliance at https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance

Staff personal data is processed on the basis of 'the contract of employment with staff'.

Where there is no lawful basis to process data the explicit consent of the individual will be obtained and recorded.

If a project requires use of personal data a Data Protection Impact Assessment should be completed. There is a form and guidance from the Information Commissioners Office to support this process.

Data

When collecting data the following principles should be followed:

- Only collect the data required.
- Ensure data is accurate and up to date.
- Do not keep data for longer than is necessary.

Data subjects have a right to:

- Request access to any data held about them.
- Have incorrect data amended or incomplete data completed.
- Have data erased.
- Request restrictions on how their data is processed and/or object to processing.
- Request copies of their electronic data to transfer to another organisation.
- Not be subject to decisions made solely by automated means.

These rights are not absolute and there can be valid reasons why a request will not be responded to in the manner expected by the individual. Each case will be judged on its own merits and specific guidance about reasons for either refusal or a different response checked, before the response is given. Guidance on making and processing a Subject Access Request can be found in the Subject Access Request/Access to Health Records Policy.

Data Security

All staff are responsible for ensuring that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of data.

Security procedures include:

Encryption. This should be used wherever possible, but particularly on mobile devices (laptops, memory sticks etc) and for any transfers of personal data via electronic means.

Psuedonymisation. Identifying factors in any use of personal data should be kept to a minimum and replaced with pseudonym where the specific identity does not need to be used.

Regular reviews of security. Many security controls can become ineffective if they are not used appropriately, so there should be regular reviews of the effectiveness of security controls.

Entry controls. No unauthorised individuals should be allowed to enter entry-controlled areas. Unknown individuals should be challenged and visitors should be escorted at all times.

Secure storage. Any storage that contains confidential data should be locked.

Methods of disposal. Paper documents should be disposed of securely. CD-ROMS and memory sticks should be physically destroyed when no longer required. Hardware that contains or processes data should be destroyed via an appropriate secure mechanism via a reputable contractor (ideally ADISA standard).

Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they lock their computer when it is left unattended.

The company maintains a register of all computer systems and which members of staff have access to them.

All computer systems are managed by System Administrators and these roles are assigned to senior members of staff. These staff sign Privileged Access Agreements defining their responsibilities.