INFORMATION MANAGEMENT & SECURITY POLICY

1. Introduction

Korus Health needs to collect and process personal data about people with whom it deals in order to carry out its business and provide its services. Such people include but are not limited to patients, employees (present, past and prospective), suppliers and other business contacts.

The data may include identifiers such as name, address, email address, data of birth, NHS Number, National Insurance Number. It may also include private and confidential information, and special categories of personal data.

No matter how it is collected, recorded and used (e.g. on a computer or other digital media, on hardcopy, paper or images) this personal information must be dealt with properly to ensure compliance with data protection legislation – the European General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA2018) which implements the GDPR in the UK.

The lawful and proper treatment of personal information by Korus Health is extremely important to the success of our business and in order to maintain the confidence of our patients and employees. Korus Health must ensure that it processes personal information lawfully and correctly.

2. Principles

Korus Health recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Korus Health fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

Korus Health also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

Korus Health believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

Korus Health fully supports and must be able to demonstrate compliance with the six principles of the Data Protection Act, 2018 which are summarised below:

• Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals;

• Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

• Personal data processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

• Personal data shall be accurate and, where necessary, kept up to date;

• Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

• Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Patients have a right to request that their confidential information is not used beyond their own care and treatment.

2.1. Openness

- Non-confidential information on Korus Health and its services should be available to the public through a variety of media, in line with the company's code of openness
- Korus Health will establish and maintain policies to ensure compliance with the Freedom of Information Act
- Korus Health will undertake or commission annual assessments and audits of its policies and arrangements for openness
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients
- Korus Health will have clear procedures and arrangements for handling queries from patients and the public

2.2. Legal Compliance

- Korus Health regards all identifiable personal information relating to patients as confidential
- Korus Health will undertake or commission annual assessments and audits of its compliance with legal requirements
- Korus Health regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise
- Korus Health will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law confidentiality
- Korus Health will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act)

2.3. Information Security

- Korus Health will establish and maintain policies for the effective and secure management of its information assets and resources including when significant company changes are made by maintaining our use of NHS security systems
- Korus Health will undertake or commission annual assessments and audits of its information and IT security arrangements through the NHS Data Toolkit.
- Korus Health will promote effective confidentiality and security practice to its staff through policies, procedures and training
- Korus Health will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security

2.4. **Information Quality Assurance**

- Korus Health will establish and maintain policies and procedures for information quality assurance and the effective management of records
- Korus Health will undertake or commission annual assessments and audits of its information quality and records management arrangements
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services
- Wherever possible, information quality should be assured at the point of collection
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- Korus Health will promote information quality and effective records management through policies, procedures/user manuals and training

3. Company Responsibilities

3.1 Appoint a Data Protection Officer (DPO) who will be responsible for providing advice, monitoring compliance and is the first point of contact in the organisation for data protection matters. The DPO reports to the Information Commissioner's Office (ICO) and directly to the governance committee.

3.2 Provide training for all staff members who handle personal information and ensure access to further guidance and support

3.3. Provide clear lines of compliance of report and supervision for compliance with data protection

3.4. Develop and maintain procedures to ensure compliance with data protection legislation, to cover for example:

3.5 IG Toolkit, managing responses to subjects' rights requests

3.6 Management of personal data breaches

3.7 Provision of privacy information

3.8 Maintain a record of processing activities

3.9 Ensure the organisation complies with its transparency and fair processing obligations in relation to data subjects' personal data

4. Employee Responsibilities

All employees will, through appropriate training and responsible management:

4.1 Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information.

4.2 Understand fully the purposes for which Korus Health uses personal information.

4.3 Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by Korus Health to meet its service needs or legal requirements.

4.4 Ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required. Paper copies through the office shredding. Digital files used for registering or appointment purposes to be removed from computers daily.

4.5 On receipt of a request by or on behalf of an individual for information held about them, or any other data subject's rights in relation to their personal data, staff will immediately notify the DPO to act according to the procedure for managing personal data requests.

4.6 Understand that breaches of this policy may result in disciplinary action, up to and including dismissal.

5. Distribution and Implementation

5.1 This document will be made available to all staff via the Korus Health website.

5.2 A training needs analysis will be undertaken with staff affected by this document by the Data Protection Officer/HR manager during staff 1:1's. Based on the findings of that analysis appropriate training will be provided to staff as necessary.

5.3 Monitoring compliance with the policies and procedures laid down in this document will be monitored via the Data Protection Officer and the governance team.

6. Information access workflow

What is a subject access request (SAR)?

By law, people can ask you for a copy of any information that's to do with them. It might be saved on your system, but if it's about them, it's their personal data, and they have a right to see it. If they ask you for a copy of it, by phone, in person, or in writing, they have made a 'subject access request' (SAR), and you need to take action.

How we deal with a subject access request

6.1 Forward the SAR to Leigh-Ann Tyler who is the Data Protection Officer as soon as it is received.

6.2 We will confirm that we have received the request and verify the identity of the requester will be verified. If the SAR is made by someone other than the person the data is about (such as a friend, relative or solicitor), we will check that they are allowed to have it. We will need to see that they have written authority to act on behalf of the person concerned, or a document showing general power of attorney.

6.3 We will send the requested information within the legally set timeframe of 1 calendar month. If it is a very complex request, we may ask to add 2 calendar months to this timeframe before the end of the first calendar month.

6.4 We will contact the enquirer to confirm the data they are requesting.

6.5 We will conduct the search for the required information from our records. For medical reasons, we routinely contact the patient's GP/referrer to gain their approval to share scan reports and/or images with the patient.

6.6 We may need to redact some information that does not relate to the enquirer in order to protect the privacy of someone else.

6.7 We will prepare and send our reply and keep a record of what we have sent.

7. Associated policies

- Confidentiality policy
- Company Privacy policy
- Acceptable Use of ICT and User Obligations
- Records Management Policy