CONFIDENTIALITY POLICY

1. Introduction

The purpose of this Confidentiality Policy is to lay down the principles that all who work within and alongside Korus Health with access to person-identifiable information or confidential information must observe.

All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and data protection legislation – the European General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA2018) which implements the GDPR in the UK.

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.

This policy sets out the requirements placed on all staff when sharing information within the NHS and between NHS and non-NHS organisations.

Confidential Information includes patient information, employee records, occupational health records as well as confidential business information

2. Principles

Caldicott Principles

Korus Health only stores and uses patient data in accordance with national guidelines and the Caldicott Principles necessary to undertake its obligations. Only the minimum and relevant patient data to a clinician's referral will be used, processed and stored in keeping with the Caldicott Principles.

The Caldicott Principles - Revised September 2013

Principle 1 - Justify the purpose(s) for using confidential informationEvery proposed use or transfer of personal confidential data within or from an organisation should beclearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - Don't use personal confidential data unless it is absolutely necessaryPersonal confidential data items should not be included unless it is essential for the specifiedpurpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential dataWhere use of personal confidential data is considered to be essential, the inclusion of each individualitem of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis. Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of
their responsibilities Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law. Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8 – Inform patients and service users about how their confidential information is usedA range of steps should be taken to ensure no surprises for patients and service users, so they canhave clear expectations about how and why their confidential information is used, and what choicesthey have about this. These steps will vary depending on the use: as a minimum, this should includeproviding accessible, relevant and appropriate information – in some cases, greater engagement will be required.

3. Responsibilities

It is the role of the Korus Health board to define Korus Health's policy in respect of information governance, taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

The governance committee is responsible for appointing appropriate officers and overseeing the day to day information governance issues; developing and maintaining policies, standards, procedures and guidance, and

monitoring awareness and compliance with the information governance policies and procedures.

The Directors within Korus Health are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is ongoing compliance.

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

A Data Protection Officer (DPO) will be assigned to provide advice to the highest level of the organisation and

all of its employees on data protection issues which can include confidentiality issues which would be reviewed in collaboration with the Caldicott Guardian as appropriate to ensure the organisation's compliance with data protection law.

The HR Manager will be responsible for ensuring that the contracts of all staff (permanent and temporary) are compliant with the requirements of the policy and that confidentiality is included in corporate inductions for all staff.

The HR Manager is responsible for ensuring the policy is kept up to date, providing advice on request to any member of staff on the issues covered within it, and ensuring that training is provided for all staff groups to further their understanding of the principles and their application.

The management team is responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon via the Information Security Incident Reporting Procedure.

4. Disclosing Personal/Confidential Information

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it. It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

5. Working in the office environment

All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents.
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended.
- Share passwords for computer systems to any other person.
- Access their own data to that of friends or family.

6. Working away from the office environment

The same principles of confidentiality apply when working away from the office environment.

To ensure safety of confidential information staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential

information must be safeguarded at all times and kept in lockable locations.

Staff must ensure that information used outside of the office is kept secure and confidential is not left unattended at any time.

Staff must not forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not use or store person-identifiable or confidential information on a privately-owned computer or device.

7. Leaving employment

On leaving employment, it is the duty of each employee to return any confidential material in his or her possession. The employee should discuss with a director any material that maybe considered confidential. Such material identified by the director as confidential must be returned before their last day of employment.

These restrictions/responsibilities also apply after the termination of employment and will only cease to apply if information has come into the public domain lawfully via proper channels.

8. Distribution and Implementation

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

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.

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

9. Associated policies

- Information Governance and Data Protection Policy
- Acceptable Use of ICT and User Obligations
- Records Management Policy
- Company Privacy Policy

Confidentiality Agreement – Korus Health

I hereby undertake not to divulge to any person, whether employed by Korus Health Ltd or not, any information I may obtain about patients or Korus Health Ltd, other than that required for the performance of my duties as an employee of Korus Health Ltd.

I accept the patient's right to confidentiality and my responsibilities for the security of health records, computerised systems and company information as outlined in this policy.

This undertaking binds me during my employment with Korus Health and also after the termination of employment.

Signed ……

Print Name ……..

Date ……..