

INFORMATION GOVERNANCE POLICY

INTRODUCTION

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management. It is therefore of paramount importance that information is efficiently managed, and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

PURPOSE OF THE POLICY

This Information Governance policy provides an overview of the practice's approach to information governance; a guide to the procedures in use; and details about the IG management structures within general practice.

THE PRACTICE'S APPROACH TO INFORMATION GOVERNANCE

There are 4 key interlinked strands to the information governance policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

Openness

- Non-confidential information on the Practice and its services should be available to the public through a variety of media, in line with the Practice's code of openness
- The Practice has policies to ensure compliance with the Freedom of Information Act
- The Practice 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
- The Practice will have clear procedures and arrangements for liaison with the press and broadcasting media
- The Practice will have clear procedures and arrangements for handling queries from patients and the public

Legal Compliance

- The Practice regards all identifiable personal information relating to patients as confidential
- The Practice will undertake or commission annual assessments and audits of its compliance with legal requirements
- The Practice regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise
- The Practice will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law confidentiality
- The Practice 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)

Information Security

- The Practice will establish and maintain policies for the effective and secure management of its information assets and resources
- The Practice will undertake or commission annual assessments and audits of its information and IT security arrangements
- The Practice will promote effective confidentiality and security practice to its staff through policies, procedures and training
- The Practice will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security

Information Quality Assurance

- The Practice will establish and maintain policies and procedures for information quality assurance and the effective management of records
- The Practice 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.
- The Practice will promote information quality and effective records management through policies, procedures/user manuals and training

PROCEDURES IN USE IN THE PRACTICE

This Information Governance policy is underpinned by the following procedures:

- **Records management procedure** that sets out how patient medical records will be created, used, stored and disposed of;
- **Access control procedure** that sets out procedures for the management of access to computer-based information systems;
- **Information handling procedure** that sets out procedures around the transfer of confidential information;
- **Incident management procedure** that sets out the procedures for managing and reporting information incidents;
- **Business continuity plan** that sets out the procedures in the event of a security failure or disaster affecting computer systems.

STAFF GUIDANCE IN USE IN THE PRACTICE

Staff compliance with the procedures is supported by the following guidance materials:

- **Records management:** guidelines on good record keeping;
- **Staff confidentiality code of conduct:** sets out the required standards to maintain the confidentiality of patient information; obligations around the disclosure of information and appropriately obtaining patient consent;
- **Access control:** guidelines on the appropriate use of computer systems;
- **Information handling:** guidelines on the secure use of patient information;
- **Using mobile computing devices:** guidelines on maintaining confidentiality and security when working with portable or removable computer equipment;
- **Information incidents:** guidelines on identifying and reporting information incidents.

RESPONSIBILITIES AND ACCOUNTABILITIES

The designated **Information Governance lead** for the practice is **Dr C Simo**. The responsibilities and accountabilities are delegated through the Practice Manager.

The key responsibilities of the lead are:

Developing and implementing IG procedures and processes for the practice;

Raising awareness and providing advice and guidelines about IG to all staff;

Ensuring that all practice staff attend Information Governance training, on an annual basis;

Co-ordinating the activities of any other practice staff given data protection, confidentiality, information quality, records management and Freedom of Information responsibilities;

Ensuring that patient data is kept secure and that all data flows, internal and external are periodically checked against the Caldicott Principles;

Monitoring information handling in the practice to ensure compliance with law, guidance and practice procedures;

Ensuring patients are appropriately informed about the practice's information handling activities.

The day to day responsibilities for providing guidance to staff will be undertaken by **Vicki Rowe**.

The **partners** of the practice are responsible for ensuring that sufficient resources are provided to support the effective implementation of IG in order to ensure compliance with the law, professional codes of conduct and the NHS information governance assurance framework.

All **staff**, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of and comply with the requirements of this policy and the procedures and guidelines produced to support it.

PRACTICE MANAGER RESPONSIBILITIES

- The Practice Manager has the responsibility for information governance at the practice.
- The Practice Manager has the responsibility for producing an IG policy.
- The Practice Manager has the responsibility for arranging information governance training (through St Helens & Knowsley NHS Trust) for all practice staff.
- The Practice Manager has the responsibility of developing a plan to ensure Smartcard users at the practice comply with the terms and conditions of use.
- The Practice Manager has the responsibility for producing and maintaining an information asset register at the practice.
- The Practice Manager has the responsibility for leading the management and reporting of information incidents.

APPROVAL

This policy has been approved by the undersigned and will be reviewed on an annual basis.

Name	Dr C Simo
Date approved	12.3.18
Review done	February 2018
Next review date	February 2021



Signed:
Dr C Simo (Information Governance Lead)

Date: **12.3.18**