Ephedra Healthcare
your local health professionals

Enhanced Access
INFORMATION GOVERNANCE POLICY

1. Summary

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 to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

2. Principles

The service recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The service 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. Enhanced Access 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.

Enhanced Access believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of everyone in the Service to ensure and promote the quality of information and to actively use information in decision making processes.

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

- Openness
- Legal compliance
- Information security
- Quality assurance

2.1. Openness

- Non-confidential information about the service and its services should be available to the public through a variety of media, in line with Enhanced Access's code of openness.
- The service will establish and maintain policies to ensure compliance with the Freedom of Information Act.
- The service 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 service has updated their privacy policy in accordance with the new regulations under GDPR on 25th May 2018.
- Data Protection Impact Assessments (DPIA's) will be carried out to minimise risks and assess whether or not remaining risks are justified. Notes on this are provided by the ICO.
- The service will ensure that the updated privacy notice is renewed annually and published on the Ephedra's web-site.
- The service will have clear procedures and arrangements for liaison with the press and broadcasting media
- The service will have clear procedures and arrangements for handling queries from patients and the public

2.2. Legal Compliance

- The service regards all person identifiable information, including that relating to patients as confidential
- The service will undertake or commission annual assessments and audits of its compliance with legal requirements in accordance with the new legislation under GDPR.
- The Service regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise. The Service will provide all members of staff with an employee privacy notice which should be signed to corroborate that they have been informed and understand why certain personal information is held by the Practice
- The Service will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law confidentiality. These will be updated and reviewed with any new legislation
- The Service 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) and the new GDPR legislation May 25th 2018.
- The Service will also appoint a named and suitably qualified Data Protection Officer (DPO). The DPO will be officially registered with the ICO and will ensure that they are kept up to date with any new guidelines or legislation
- The Service will continue to have a Caldicott Guardian who will remain officially registered and will also attend regular training.

2.3. Information Security

- The Service will establish and maintain policies for the effective and secure management of its information assets and resources
- The Service will undertake or commission annual assessments and audits of its information and IT security arrangements
- The Service will promote effective confidentiality and security practice to its staff through policies, procedures and training. All members of the Service will have to complete the GDPR training module on Bluestream Academy as mandatory. They will also all be given an employee's privacy statement to read and sign to ensure they all understand the implications of Data protection and privacy etc.
- The Service will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security. All breaches will now be reported to the ICO in accordance with their guidelines. This can be either by phone or an emailed template. The template is on the ICO web-site.

2.4. Information Quality Assurance

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

3. Responsibilities

It is the role of the Clinical Director within Ephedra to define the policy in respect of Information Governance, taking into account legal and NHS requirements. The Clinical Director is also responsible for ensuring that sufficient resources are available to support the requirements of the policy.

The Information Governance Lead for the Enhanced Access Service within Spring House is Natalie Cox and Dr Royce Abrahams is our Caldicott Guardian and therefore is also the Practice's Data Controller. Natalie Cox is also the appointed DPO. Both DPO and Caldicott Guardian will ensure they both attend regular updates and complete the Bluestream modules annually.

The designated Information Governance Lead in the Service is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the Practice, raising awareness of Information Governance and ensuring that there is ongoing compliance with the policy and its supporting standards and guidelines.

4. Policy Approval

The Service acknowledges that information is a valuable asset, therefore, it is wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed, protecting the interests of all of its stakeholders.

This policy, and its supporting standards and work instruction, are fully endorsed by the CCG through the production of these documents and their formal approval by the Practice.

We will, therefore, ensure that all staff, contractors and other relevant parties observe this policy in order to ensure compliance with Information Governance and contribute to the achievement of the Service objectives and delivery of effective healthcare to the local population.

Practice Manager _____

Date _____

Caldicott Guardian _____

Date _____

Enhanced Access Clinical Director _____

Date _____