INFORMATION GOVERNANCE POLICY

The purpose of this policy is to provide the Chevin Medical Practice (The Practice) staff with a framework in regards to Information Governance.

The policy has been developed and reviewed in line with developments within the Information Governance agenda, Pseudonymisation and the Information Governance Toolkit.

Legislation

- Data Protection Act 2018
- General Data Protection Regulation 2016
- Human Rights Act 1998
- Freedom of Information 2000
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act)
- Computer Misuse Act
- Copyright, designs and patents Act 1988 (as amended by the - Copyright Computer programs regulations 1992)
- Crime and Disorder Act
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Common Law Duty of Confidentiality
- National Health Service Act 1977

The policy provides a balance between the openness and confidentiality in the management and use of information. This policy provides a standard to which information should be dealt with to abide by legal obligations. The policy states that all personal identifiable information relating to patients and staff as confidential, except where national policy on accountability and openness requires otherwise.

This Policy will be reviewed annually by the Information Governance Practice Lead in line with the NHS Digital Data Security and Protections Toolkit and any new guidance or changes within procedure.

Distribution
This policy will be available for all staff to view on the practice's Intranet. Managers of staff without direct access to the practice's Intranet must provide access to an up to date paper copy of the policy.

1.0 Introduction

1.1 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.

1.2 It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

1.3 Information Governance is a framework in which information should be handled in accordance with legal and ethical standards. This policy provides staff with how this framework can be achieved within the Organisation.

2.0 Purpose of the Policy

2.1 To ensure the practice meets its responsibility for the legal and ethical management of information assets and resources and ultimate compliance with the Information Governance Toolkit, NHS and other professional Codes of Conduct relating to confidentiality and consent; guidance from the Information Commissioner.

3.0 Policy Aim

3.1 The aim of this policy is to provide the employees of the practice with a simple framework through which the elements of Information Governance will be met.

3.2 The practice aims to achieve a standard of excellence of Information Governance by ensuring that information is dealt with legally, securely and effectively in the course of the practice business in order to deliver high quality patient care.

4.0 Scope

4.1 Information Governance covers all staff employed by the practice, private contractors, volunteers and temporary staff. The scope is:

- All information recorded, disclosed and used by the practice.
- All information systems managed by the practice
- Any individuals using information “owned” by the practice
- Any individuals requiring access to information “owned” by the practice

5.0 Policy Principles

5.1 The Practice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The practice 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, staff and commercially sensitive

information. The Practice also recognises the need to share patient's 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.

5.2 The Practice 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, managers and staff to ensure and promote the quality of information and to actively use information in decision making processes.

5.3 There are 4 key interlinked strands to the Information Governance Policy:

- Openness
- Legal Compliance
- Information Security
- Quality Assurance

6.0 Openness

6.1 Information will be defined as, and where appropriate kept, confidential underpinning the principles of Information Governance and the provisions of in the General Data Protection Regulation 2016 and Data Protection Act 2018..

6.2 Non-confidential information and services will be available to the public through a variety of means including the practice's internet based Publication Schemes under the Freedom of Information Act 2000.

6.3 The Practice must ensure compliance with the Freedom of Information Act 2000 and will favour the disclosure of requested information.

6.4 Patients will have access to information relating to their own health care, options for treatment and their rights as patients. Any request for access to personal information by the patient or the patient's representative must be processed in line with the practice's Subject Access Request procedures. The Practice must ensure compliance with the GDPR 2016,Data Protection Act 2018, the Freedom of Information Act 2000 and the Access to Health Records Act 1990 (in relation to deceased patient's records).

6.5 The Practice will have clear procedures and arrangements for liaison with the press and broadcasting media.

6.6 Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.

6.7 Availability of information for operational purposes will be maintained and within set parameters relating to its importance via appropriate procedures and computer system resilience.

6.8 Compliance with legal and regulatory framework will be achieved, monitored and maintained through the Information Governance Toolkit and associated procedures. .

6.9 The Practice will establish and maintain policies and procedures to ensure compliance with the Data Protection Act 1998, Human Rights Act 1998, the common law duty of confidentiality and the Freedom of Information Act 2000 and all forthcoming related legislation.

7.0 Legal Compliance

7.1 The Practice will regard all personal confidential information relating to patients and staff as confidential, except where national policy on accountability and openness requires otherwise.

7.2 The Practice will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking into account relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

7.3 The Practice will undertake annual assessments and audits of its compliance with legal requirements.

7.4 The Practice will establish and maintain policies to ensure compliance with the Data Protection law, Human Rights Act and the common law duty of confidentiality.

8.0 Information Security

8.1 The Practice will establish and maintain procedures for the effective and secure management of its information assets and resources.

8.2 The Practice will undertake annual assessments and audits of its information and IT security arrangements.

8.3 The Practice will promote effective confidentiality and security practice to its staff through policies, procedures and training.

8.4 The Practice must maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

9.0 Information Quality Assurance

9.1 The Practice will establish and maintain procedures for information quality assurance and the effective management of records.

9.2 The Practice will undertake annual assessments and audits of its information quality and records management arrangements.

9.3 Wherever possible information quality should be assured at the point of collection.

9.4 Data standards will be set through clear and consistent definition of data items in accordance with national standards.

9.5 The Practice will promote information quality and effective records management through a range of policies, procedures/user manuals and training.

10.0 Management of Information Governance

10.1 The management of Information Governance across the practice will be co-ordinated by the Information Governance Lead.

10.2. The Data Security and Protections toolkit

The DS&P covers all aspects of legal compliance and encompasses the following initiatives:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance

10.3 In order to successfully implement this programme it has been recognised that robust Information Governance arrangements are required. Information governance covers the information component of both Clinical Governance and Corporate Governance and provides a framework for handling information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service.

10.4 It looks at the systems and access rights to which staff and managers have access, and the way in which information is shared.

10.5 The implementation of the IG Policy and the DS&P toolkit will ensure that information is more effectively managed within the practice.

10.76 The year on year improvement plans taken from the practice's scoring of the IG Toolkit will show improvement and/or maintenance of the high standards reached.

10.87 To enforce the Care Record Guarantee and ensure compliance with the NHS 12 commitments:
http://www.connectingforhealth.nhs.uk/newsroom/news-stories/crdb_guarantee.

11.0 Responsibilities

11.1 *Organisational Responsibilities*

11.1.1 All information recorded and subsequently used / handled by NHS staff is subject to consent from the Individual to whom the data relates. The practice ensures that all staff members are clear about their legal and ethical responsibilities relating to data recording and usage, and ensures and supports appropriate education and training.

11.1.2 The practice must ensure that legal and ethical requirements relating to information are met.

11.1.3 The practice must make arrangements to meet the performance assessed requirements of the Connecting for Health IG Toolkit which ultimately feeds into other external assessments, e.g. Care Quality Commission.

11.2 *Responsibilities of Staff*

11.2.1 Recorders and users of information must:

- Be aware of their responsibilities
- Complete Information Governance training annually
- Comply with policies and procedures issued by the practice
- Report all information governance incidents
- Work within the principles outlined in the information governance toolkit, relevance NHS Codes and guidelines produced by e.g. Information Commissioner.

12.0 Training

12.1 Fundamental to the success of delivering the IG Policy is developing an IG culture within the practice. Awareness and training must be provided on an ongoing basis to all staff to promote this culture.

12.2 All new staff must receive training as part of the practice's Induction on Data Protection, Confidentiality, Security, Freedom of Information and Records Management.

12.3 Information Governance Training is mandatory for staff and can be completed via the on-line training modules or within a face to face training session provided by PCIG Consulting Limited where particular needs have been identified. Training is required annually for all staff which ensures they are kept up to date with any changes.

12.4 The Practice awareness sessions and campaigns are also planned.

13.0 References

13.1 *Legal and Regulatory Framework*

13.1.1 The Practice is bound by the provisions of a number of items of legislation and regulation affecting the stewardship and control of information. The main relevant legislation are regulations are:

- Data Protection Act 2018
- General Data Protection Regulation 2016
- Human Rights Act 1998
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Information Governance Policy Page 12 of 53 December 2009
- Copyright (Computer Programs) Regulations 1992
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- Health and Social Care Act
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations)
- Public Interest Disclosure Act 1998
- NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000
- Human Fertilisation and Embryology Act 1990
- Abortion Regulations 1991
- Public Records Act 1958
- Regulations under the Health and Safety at Work Act 1974
- Re-use of Public Sector Information Regulations 2005

13.1.2 This list is not exhaustive.

13.2 *Regulatory Framework*

13.2.1 In relation to many of the above, the NHS has set out and mandated a number of elements of regulation that constitute “Information Governance” through a national programme. This area is developing at a fast changing pace and the focus within this section will need significant periodical review. The Regulatory Elements are:

- DS&P Toolkit which requires practicess to assess their progress against set criteria
- Caldicott – a report for the audit and improvement on the use of patient identifiable data (1997) and HSC 1999/012
- Standards for Information Security Management
- Information Quality Assurance
- NHS Confidentiality : Code of Practice (2003)
- NHS Guidance on Consent to Treatment
- Records Management: NHS Code of Practice
- Care Quality Commission Regulations
- Information Commissioner

- Caldicott Principles

13.3 *Ethical framework*

13.3.1 The right to expect privacy ethically entitles a patient to the exercise of control over the content, uses of and disclosures of information about them as an individual. Respect for that privacy by staff is essential for maintaining patient trust in, and integrity of, the relationship between staff and patient. The Department of Health provides basic principles that underpin ethical frameworks and which form part of staff work practices in implementing this policy. These are:

13.3.2 Staff should:

- Protect – look after patient's information
- Inform – ensure patients are aware of how their information is used; there should be no surprises
- Provide Choice – allow patients to decide whether their information can be disclosed and used in particular ways.
- Improve practice – by always looking for better ways to protect, inform and provide choice.

13.3.3 So that the public/patient will

- Understand the reasons for recording and processing information
- Give their consent for the disclosure and use of their personal information
- Gain trust in the way the NHS handles information
- Understand their rights to access information held about them

13.3.4 The Caldicott principles, applying to the disclosing of patient-identifiable information, are:

- Justify the purpose(s) of every proposed use or transfer
- Don't use it unless it is absolutely necessary, and
- Use the minimum amount of patient identifiable data necessary
- Access to it should be on a strict need-to-know basis
- Everyone with access to it should be aware of their responsibilities, and
- Understand and comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality

13.4 *Information Commissioner*

13.4.1 The Information Commissioner has specific responsibilities under the GDPR 2016. This Regulation provides a framework to ensure that personal information is handled properly. The Act works in two ways:

13.4.2 Firstly, it states that anyone who processes personal information must comply with 6 principles, which make sure that personal information is:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) 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 may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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."

13.4.3 Secondly, the Regulation provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

13.4.4 Additionally, all staff should be familiar with their own professional codes relating to ethical aspects of information governance (i.e. respect for patient privacy and dignity).

14.0 Monitoring Compliance

14.1 Staff are expected to comply with the requirements set out within the Information Governance Policy and related policies. Compliance will be monitored via the practice IG Lead reports of spot checks, completion of staff questionnaires, incidents reported, electronic audit trails and submission of the Information Governance Toolkit.

14.2 Non-adherence to the Information Governance Policy and related policies will result in local Disciplinary Policies being implemented