Dr. Rafaqat Rashid
MBChB, MA

Dr. Amar m. Bostan
MBChB, MRCP, MRCGP

PICTON MEDICAL CENTRE

http://www.pictonmedicalcentre.nhs.uk

Westbourne Green Community
Health Care Centre
50 Heaton Road
Bradford
West Yorkshire
BD8 8RA
Tel: (01274) 019605
Fax: (01274) 019610

Information Governance Policy

Version:	Review date:	Edited by:	Approved by:	Comments:
1	28.1.2020	Rebekah Harrison	Anne-Marie Mitchell	

CONTENTS

4.4. Information Quality Assurance

5. Roles and Responsibilities

6. What to do in breach of the policy

7. References

APPENDIX A

1. Introduction

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources.

Information plays a key part in clinical governance, service planning and performance management and therefore it is essential that we as a Practice, ensure information is:

• Held securely and confidentially,
• Obtained fairly and efficiently,
• Recorded accurately and reliably,
• Used effectively and ethically, and
• Shared appropriately and lawfully.

Information Governance provides an overarching, consistent and robust framework for the practice to manage the many different information-handling requirements necessary for the effective delivery of primary care, whilst ensuring the protection of personal and sensitive information provided by both patients and staff.

2. Details of application

This policy covers all aspects of information within the practice, including (but not limited to):

• Patient/Client/Service User information,
• Personnel information, and
• Organisational information.

This policy covers all aspects of handling information, including (but not limited to):

• Structured record systems – paper and electronic
• The transfer of information – fax, e-mail, post and telephone

All information systems purchased, developed and managed by/ or on behalf of, the Practice and any individual directly employed or otherwise are covered by this policy.

3. Summary /Policy Statement

PMC recognises the need for an appropriate balance between openness and confidentiality in the management, storage and use of information, and fully supports the principles of corporate governance, whilst recognising public accountability. The Practice places significant importance on the confidentiality of, and the security arrangements required, to safeguard both personal information (staff and patients) and commercially sensitive information, yet 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 specific circumstances, the public.

The Practice believes that accurate, up-to-date and relevant information is essential for the delivery of high quality healthcare. It is therefore the responsibility of all clinicians, managers and staff to ensure and promote data quality and maintain effective and accurate audit trails.

By following the key principles of Information Governance staff and patients can be reassured that:

• Records will not be disclosed inappropriately, thereby strengthening trust and belief in NHS working practices,
• Openness will be encouraged; thereby patients and staff can be confident when sharing important and relevant, yet personal information, and

• They will receive the best quality care and support they require.
This policy complies with the following legal acts and the NHS regulation framework.

3.1. Legal Acts

The organisation is bound by the provisions of a number of items of legislation affecting the stewardship and control of information. This includes the:

• Data Protection Act 1998
• Freedom of Information Act 2000
• Environmental Information Regulations 2004
• Human Rights Act 1998
• Regulation of Investigatory Powers Act 2000 (& Lawful Business Practice Regulations 2000)
• Crime & Disorder Act 1998
• Criminal Justice Act 2003
• Computer Misuse Act 1990
• Access to Health records Act 1990 (where not superseded by the Data Protection Act 1998)
• Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992)
• Electronic Communications Act 2000
• Children Act 1989
• NHS & Community Care Act 1990
• Mental Health Act 1983

• Carers (Recognition & Service) Act 1995
• Service Users Access to Records Act 1987 & Regulations 1989
• Adoption and Children Act 2002
• Health Act 1999 (Section 31)
• Health and Social Care Act 2001

This policy also describes the way in which information should be managed - in particular, the way in which personal or sensitive information should be protected. In addition to the above, the following additional legislation could also impact upon the way in which information is used:

• Public Interest Disclosure Act 1998
• Audit & Internal Control Act 1987
• NHS Sexually Transmitted Disease Regulations 2000
• National Health Service Act 1977
• Human Fertilisation & Embryology Act 1990
• Abortion Regulations 1991
• Prevention of Terrorism (Temporary Provisions) Act 1989 & Terrorism Act 2000
• Road Traffic Act 1988
• Regulations under Health & Safety at Work Act 1974

3.2. NHS Regulatory Framework

In relation to many of the above requirements, the NHS set out and mandated a number of elements of regulation that constitute 'Information Governance'. This area of work is constantly developing and therefore the focus within this section will be reviewed appropriately in line with the release of further guidance from the Department of Health. The regulation elements are:

• Caldicott – Report, audit & improvement on the use of Patient Identifiable Data
• ISO17799 – British Standard for Information Security Management, mandated for the NHS in 2001
• Data Accreditation
• PRIMIS Data Quality

The above also impact on, and can be incorporated within, a number of wider NHS regulation elements, namely:

• The Annual Health Check and Standards for Better Health (monitored by the Healthcare Commission)
• Clinical Negligence Scheme for Trusts (CNST)
• NHSLA Risk Management Standards

4. Principles

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

• Openness
• Legal compliance
• Information security

• Quality assurance

4.1. Openness

The Code of Practice on Openness in the NHS represents the government's intention to ensure greater access by the public to information about public services, thereby encouraging and improving mutual confidence between the NHS and the public. The intentions of the code are also supported by the principles of the Freedom of Information Act 2000 and include:

• 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 ensures compliance with the Freedom of Information Act 2000, Environmental Information Regulations 2004, the Data Protection Act 1998 and the Access to Health records Act 1990 (where not superseded by the Data Protection Act 1998).
• Patients will have access to information relating to their own health care, their options for treatment and their rights as patients
• The Practice will ensure that there are clear and effective arrangements to deal with complaints and concerns about services and access to information, and that these procedures are widely publicised and effectively monitored.

4.2. Legal Compliance

As highlighted under Section 3.1, Legal Acts, the Practice is bound by the obligations and requirements of the Acts listed and therefore will adopt the following principles:

• The Practice regards all identifiable personal information relating to patients as confidential and complies with the principles of Caldicott and the Data Protection Act 1998.
• The Practice will establish and maintain policies to ensure compliance with the required Legal Acts and control and monitor the 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)

4.3. Information Security

The Critical National Infrastructure (CNI) protection programme works with organisations to ensure that services that need to be secured from electronic attack are protected in a way that is proportional to the threat. As part of the CNI community, the NHS must therefore operate and manage its information systems, networks and services such that they are appropriately protected. The Heaton Medical Practice therefore ensure that:

• Policies for the effective and secure management of all information assets and resources will be established and maintained.

• Effective confidentiality and security practice is promoted to all staff through up-to-date policies and procedures. Staff responsibilities with regard to information governance issues will be routinely assessed and additional training provided as required.
• Appropriate incident reporting procedures and reported instances of actual or potential breaches of confidentiality and security will be monitored and maintained.
• Information Assets and information flows will be mapped and recorded to assess and prevent the unlawful and unnecessary use of person identifiable information.

4.4. Information Quality Assurance

Information Quality Assurance aims to assess performance and deliver improvement in relation to both the quality of information but also, as a means of developing and reinforcing an information quality culture. Information Quality Assurance involves understanding organisational structures, creating appropriate management structures, identifying process, applying standards, assessing performance and providing guidelines to enable and sustain performance. The Practice will therefore:

• Establish and maintain policies and procedures for information quality assurance and the effective management of records;
• Take ownership of, and seek to improve, the quality of information within the practice;
• Promote information quality at the point of collection;
• Set clear and consistent definitions of data items, in accordance with national standards, and
• Promote information quality and effective records management through policies, procedures/user manuals and training programmes.

5. Roles and Responsibilities

All staff, whether permanent, temporary or contracted 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. Managers are also responsible for promoting this policy and ensuring compliance by their team members.

6. What to do in breach of the policy

All breaches of the policy should be reported to the Practice Manager where she will then take any necessary action required.

7. References

• The Code of Practice on Openness in the NHS
• The draft strategy for Information Quality Assurance (Information Policy Unit, Department of Health)

• NHS Information Authority Guidance on Information Governance Toolkit (Requirement IG Management, Seq 903)
• The NHS Confidentiality Code of Practice
• www.connectingforhealth.nhs.uk
• www.doh.gov.uk
• www.informatics.nhs.uk

APPENDIX A

SUPPORTING PRACTICE POLICIES AND PROCEDURES

- Data Protection Policy
- Freedom of Information Policy
- Records Management Policy
- Confidentiality Agreement
- Access to Health Records Protocol