

City & Hackney Information governance policy

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 provide a robust governance framework for information management.

Principles

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 and staff and commercially sensitive information. The Practice 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.

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 and managers 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

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 will establish and maintain 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

PRINCIPLES IN THE USE OF CONFIDENTIAL INFORMATION – CALDICOTT GUIDELINES

The purpose of this section is to outline a local code of conduct on the use of confidential information to ensure that patient or personal identifiable data is used and disclosed in an adequate manner according to the Caldicott Principles Data Protection Act and the Freedom of Information Act. The Practice has appointed a Caldicott Guardian: **Katie O'Beirne** is the Caldicott Guardian for the Practice.

All Practice Staff, both clinical and non-clinical must adhere to all Policies and Procedures concerning Information Governance and Confidentiality.

CONFIDENTIALITY POLICY

The practice has a comprehensive confidentiality policy which is mandatory reading for new employees and on the staff reading list.

This policy covers areas including all aspects of communication including verbal, email, written documents, faxing both in and outgoing and post.

It also covers issues relating to working away from the office, and the principles of maintaining confidentiality and management of confidential waste, internet use and maintenance and security of passwords.

The policy refers to relevant legal tools and the practice's right to monitor use of the internet.

The policy gives staff information of how to report breaches in confidentiality or information governance.

The policy covers user of email, including etiquette, offensive emails and confidentiality.

FIREWALL AND VIRUS PROTECTION

The Firewall and Virus Protection of the computer system is the responsibility of NELCSU, who maintain the Practice IT systems.

ANTIVIRUS

The Internet is a major source of computer viruses the effects of which can range from a minor irritant to a major disaster and all have costs involved in their eradication.

Although the IT network has background antivirus defences it is still essential for users to specifically check files and mail prior to opening. In the event that a user suspects a virus infestation they must stop using that machine, and contact the IT Help Desk.

TRAINING

All staff will be given training on information governance and confidentiality at induction and as part of the ongoing training schedule. If a member of staff requires further training they will discuss this with the practice manager. Staff with line management responsibility should ensure that the staff working for them are aware of the above principles and make training available if required.

SECURITY BREACHES

An Information Security incident is defined as any event which has resulted, or could result in:

1. the disclosure of confidential information to any unauthorised individual
2. the integrity of the system or data being put at risk
3. the availability of the system or information being put at risk
4. an adverse impact, for example: embarrassment to the NHS; threat to personal safety or privacy; legal obligation or penalty; financial loss; disruption of activities

Types of incidents that should be recorded include:

1. computer misuse;
2. computer virus activity
3. confidentiality breach
4. records related incident
5. theft or loss of records
6. System abuse or infiltration
7. This list is not exhaustive