Weobley & Staunton on Wye Surgeries

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 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.

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.

PRINCIPLES

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

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.

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

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 everyone in the Practice 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

- Information will be defined as, and where appropriate kept, confidential underpinning the principles of Information Governance and the provisions in the General Data Protection Regulation 2016 and the Data Protection Act 2018.
- 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.
- The Practice must ensure compliance with the Freedom of Information Act 2000 and will favour the disclosure of requested information.
- 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)
- The Practice will have clear procedures and arrangements for liaison with the press and broadcasting media.
- Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.
- Availability of information for operational purposes will be maintained and within set parameters relating to its importance via appropriate procedures and computer system resilience.
- Compliance with legal and regulatory framework will be achieved, monitored and maintained through the DSP Toolkit and associated procedures.
- 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.

Legal Compliance

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

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.
- 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.

Management of Information Governance

- The management of Information Governance across the Practice will be co-ordinated by the Information Governance Lead.
- The Data Security and Protections Toolkit – This covers all aspects of legal compliance and encompasses the following initiatives:

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

- 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.
- It looks at the systems and access rights to which staff and managers have access, and the way in which information is shared.
- The implementation of the Information Governance Policy and the DSP Toolkit will ensure that information is more effectively managed within the Practice.
- 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.
- The ensure the Care Record Guarantee and ensure compliance with the NHS 12 commitments: www.connectingforhealth.nhs.uk/newsroom/news-stories/crdb_guarantee

RESPONSIBILITIES

Organisational Responsibilities

- 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.
- The Practice must ensure that legal and ethical requirements relating to information are met.
- The Practice must make arrangements to meet the performance assessed requirement of the DSP Toolkit which ultimately feeds into other external assessments, eg. Care Quality Commission

Responsibilities of Staff

- 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 DSP Toolkit, relevant NHS Codes and guidelines produced by eg. Information Commissioner.

TRAINING

- 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.
- All new staff must receive training as part of the Practice's Induction on Data Protection, Confidentiality, Security, Freedom of Information and Records Management.
- Information Governance training is mandatory for staff and can be completed via the online 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 that they are kept up to date with any changes.
- The Practice awareness sessions and campaigns are also planned.

INFORMATION SECURITY & CONFIDENTIALITY

A General Practice has a legal obligation to comply with all appropriate legislation in respect of Data, Information and IT Security. It also has a duty to comply with guidance issued by the Department of Health, NHS Digital, other advisory groups to the NHS and guidance issued by professional bodies.

Information systems form a major part of the efficiency of a modern general practice. Adequate security procedures are critical in ensuring the confidentiality, integrity and availability of these systems. It is important that a general practice has an Information Governance Policy to provide management direction and support on matters of information security and confidentiality in general practice.

Connection and access to the NHS net is conditional on there being an Information Governance Policy in place. Wherever personal information is held, on paper or computer, it is subject to the eight Principles of the Data Protection Act 1998.

Individuals and the practice may be prosecuted or subject to a claim for damages for any instance where the Data Protection Principles are breached or where a person suffers loss, damage or harm from misuse of information.

Information Security comprises:

Confidentiality

Everyone involved is required to maintain the confidentiality of all data within the practice by:

- Ensuring that only authorised people can gain access to the information and systems
- Not disclosing information to anyone who has no right to know, see or be aware of it

Integrity

Everyone involved is required to maintain the integrity of all the data within the practice by:

- Taking care over input
- Checking that the correct record is on the screen before updating
- Learning how the systems should be used and keeping up to date with changes which may affect how it works
- Reporting apparent errors to the Security Lead (Practice Manager or IG Lead GP)

Availability

A nominated member of staff is required to maintain the availability of all the data by:

- Ensuring that the equipment is protected from security risks
- Ensuring that backups of the data are taken at regular intervals
- Ensuring that appropriate contingency is in place for equipment failure or theft and that these contingency plans are tested and kept up to date

PATIENT INFORMATION

Patients have a right to expect that information about them is kept confidential. The practice should use patient-identifiable information only for the individual patient's health care, for internal audit arrangements and to justify certain payments to the general practice.

Under certain circumstances, visiting computer engineers may, in the course of their work view patient-identifiable information. Such engineers must be bound by strict contractual agreements containing legal and confidentiality requirements. The Practice has produced a leaflet for members of the public informing them how the NHS and local health community uses their information. This leaflet should be displayed in prominent areas of the practice.

Data that has been anonymised such that patients cannot in any way be identified may be used by the Practice and other clinical organisations for research purposes without seeking further consent.

Apart from disclosures required by law all other uses of information will require patient consent. The NHS is working towards achieving Informed Consent where information is used for purposes other than stated above.

CALDICOTT REPORT

The Caldicott Report on Protecting and Using Patient Information was produced in December 1977 and is mandatory within the NHS.

It developed a set of good practice principles against which every flow of patient-identifiable information should be regularly justified and tested.

Caldicott Principles

- Justify the purpose(s) for using confidential information
- Only use it when absolutely necessary
- Use the minimum required
- Access to confidential information should be on a strict need to know basis
- Everyone must understand his/her responsibilities
- Everyone must understand and comply with the law

A key part of the recommendations contained within the report was the establishment of a network of Caldicott Guardians of patient information; your Practice has a nominated Guardian. Caldicott Guardians have a responsibility to develop a framework of protocols to safeguard and govern the uses made of patient information within NHS organisations. Any concerns relating to Caldicott should be made to the Information Governance Lead.

Your Caldicott Guardian is	**Dr. Tom Moore**

LEGISLATION

Legal & Regulatory Framework

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 regulations are:

- Data Protection Act 2018
- General Data Protection Regulations 2016
- Human Rights Act 1198
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Copyright, Designs and Patent Act 1988
- Copyright (Computer Programs) Regulations 1992
- Crime & Disorder Act 1998
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- Health & 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 Disease) Directions 2000
- Human Fertilisation and Embryology Act 1990
- Abortion Regulations 1991
- Public Records Act 1958
- Regulations under the Health & Safety at Work Act 1974
- Re-use of Public Sector Information Regulations 2005

This list is not exhaustive.

Regulatory Framework

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:

- DSP Toolkit which requires practices 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

Ethical Framework

- 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 look for better ways to protect, inform and provide choice

- 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

- 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

Information Commissioner

- 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:

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

    - Processed lawfully, fairly and in a transparent manner in relation to individuals
    - 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;
    - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
    - 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;
    - 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
    - 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."

  - 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.
  - 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).

COMPUTER SYSTEMS

- Practice systems must only be used for approved purposes authorised by the Partners and managed by the Security Lead, or if applicable, the IT specialist.

- Only suitably qualified or experienced staff should undertake maintenance work on, or make changes to, the practice systems

- Only authorised software may be installed and it must only be used in accordance with the software licence agreement

- Adequate documentation should be produced or made available for users as appropriate

- To maintain the integrity and availability of practice systems, back-ups of practice software and information must be taken regularly

If the internal network is connected to other services outside the practice, then additional care must be taken when using these services eg. the NHS net. The NHS net (nww) is a private network for the NHS offering information and email communications. If connected, access will be possible through this service to connect to the internet. This will enable the practice user to view (or browse) a whole range of websites and send email communications around the work. The NHS net managed service provider monitors the use of this network.

Connection to inappropriate sites on the internet, downloading or sending offensive material may lead to investigation, disconnection and possibly prosecution and disciplinary.

Any incident leading to a breach of security of the practice or information held within it must be reported to the Information Governance Lead.

PASSWORDS

- Passwords must be adequate to provide the first line in defence to unauthorised access to data or systems
- Passwords should be a minimum of 6-8 characters in length with a mixture of letters and numbers and have an expiry date
- Passwords must be changed regularly

ACCESS CONTROL

- Access must be granted to, and revoked from, information systems in a controlled manner.
- The user list must be reviewed regularly
- Leavers and those no longer requiring access for their duties must be removed from the system immediately

ANTI-VIRUS

Unless completely isolated, computer systems are continually at risk from virus infection. This risk is greater as the volume of data transferred between systems and networks increases. While most viruses are relatively harmless, they can cause serious disruption to both the user and the wider network.

Viruses may be received as:

- An email message or as an attachment to a message
- A macro within a word processor or spreadsheet document
- An infected programme that has been downloaded

If a virus is suspected, prompt action is essential – inform the Security Lead immediately. An appropriate version of anti-virus software must be installed on practice machines and receive regular updates of the 'engine' and antidote files (known as virus definition files)

TRANSMITTING PATIENT DATA

Some physical areas of the practice should be restricted and provide a 'safe haven' for the use and control of patient information.

It should not be assumed that other premises have the same level of security.

NHS net is secure for the transmission of personal or patient information as it is an encrypted network.

ASSETS/EQUIPMENT MANAGEMENT

The protection of assets is essential. Both software and hardware assets must be accounted for and a level of 'ownership' established.

Examples of assets associated with information systems are:

- Information and Data
- Software programs
- Physical Equipment, eg. practice server, desktop computers, printers & laptops
- Services

Responsibility for the security of information assets must be assigned to a named individual

General Practice assets and equipment must not be removed from the premises or lent to anyone without the permission of a Partner or the Practice Manager

MOBILE COMPUTING

Extra care must be taken when using laptops.

When connected to the Practice through external telecommunications systems a secure level of authorisation and identity must be established. This should be in accordance with the Acceptable Use Policy, Code of Connection.

These devices have an additional risk to their physical security from loss, theft or damage. Ensure that all serial number(s) of the equipment are written down.

It is strongly advised that permanent security marking/engraving is used on all equipment.

Care must be taken to ensure that the data entered remotely is transferred as soon as possible to the Practice system(s).

CLEAR DESK POLICY

The Practice should ensure that all documents and information are removed from computer screens and desktops and are correctly filed when not in use.

DISPOSAL OF INFORMATION AND EQUIPMENT

Information containing personal details no longer required must be disposed of in accordance with the corresponding legislation.

Computer disks, memory sticks and equipment that contains personal data must have that information permanently deleted or destroyed.

PHYSICAL SAFETY AND SECURITY

A General Practice will work within the requirements of the relevant Health & Safety at Work Act to maintain a safe and secure environment for its employees, patients and visitors.

Safety and security systems installed on the premises must be operated in accordance with their instructions and should not be tampered with or repaired other than by suitably competent or qualified persons.

Electrical equipment must be used in accordance with the Electricity at Work Regulations.

Suspected defects must be reported to the Security Lead as soon as possible.

A suitable forum for security issues should be available within the Practice, eg. having an agenda item at regular meetings.

All staff must have the opportunity and mechanism available to report security concerns.

MONITORING COMPLIANCE

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, incident reports, electronic audit trails and submission of the DSP Toolkit.

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

Confidentiality Notice

This document and the information contained therein is the property of **The Weobley & Staunton-On-Wye Surgeries**. This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from **The Weobley & Staunton-On-Wye Surgeries**.

Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
1.0	07.05.14	Michele Petrie	Michele Petrie	
2.0	29.01.15	Michele Petrie	Michele Petrie	Reviewed – no changes
2.0	30.12.15	Michele Petrie	Michele Petrie	Reviewed – updated with removal of Dr. Cutler
3.0	22.12.17	Michele Petrie	Michele Petrie	Updated to incorporate Information Security & Confidentiality Policy and IGSoC into one policy
4.0	11.05.18	Michele Petrie	Michele Petrie	Reviewed and updated in line with Paul Couldrey's information governance policy
5.0	29.10.18	Michele Petrie	Michele Petrie	Updating of Caldicott Guardian
5.0	22.10.19	Michele Petrie	Michele Petrie	Reviewed – No changes
5.0	20.07.22	Suzi Cox	Suzi Cox	Reviewed- updated no longer use fax machine to transmit data.

Appendix A

Relevant Acts of Parliament and NHS Guidelines and What They Mean for Employees

Requirement	What It Covers	Personal Responsibilities	Penalties for Breaches
Data Protection Act 1998	Person identifiable information about living individuals – manual and automated records (eg. on computer, video tape, digital images)	Keep all person identifiable information secure and confidential – see Code of Conduct for specific details	Unauthorised disclosure of personal identifiable information could lead to court action and a criminal conviction and/or the payment of compensation to a claimant
Human Rights Act 1998 (Article 8)	An individual's right to privacy for themselves and their family members	As above	As above
Computer Misuse Act 1990	Unauthorised access to computer held programs and information/data	Do not use any other person's access rights (eg. user ID and password) to access a computer database	A criminal record and a person sentence of up to 5 years
Common Law of Confidentiality	An individual's right to confidentiality of their information when alive and once they have died	Keep all information secure and confidential. Also remember this covers wishes of deceased persons – if it is recorded they do not want details of their treatment disclosed when they die this wish will normally need to be respected	Disciplinary Action
Caldicott	Security and confidentiality of personal health and social care information for patients and service users	See Code of Conduct for further information	Disciplinary Action
Contract of Employment	Employees responsibilities including security and confidentiality of any information accessed during the course of work	Comply with Contract of Employment and Code of Conduct	Disciplinary Action