Date published: **June 2022**
Date of review: **June 2023**

WESTOVER SURGERY

INFORMATION GOVERNANCE POLICY

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. It plays a key part in clinical governance, service planning, delivery and performance management.
- It is 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. Purpose

- To describe a system that ensures the Practice meets its responsibilities for the management of its information assets and resources. The Practice will establish and support an Information Governance Strategy.

3. Principles

- The Practice recognises the statutory and professional need for an appropriate balance between openness and confidentiality in the management and use of information.
- The Practice fully supports the principles and requirements of information governance (IG) and recognises its responsibility and public accountability, placing importance on the confidentiality and security arrangements to safeguard personal information about patients and staff.
- The Practice also recognises the need to share patient information with other health organisations and 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 managers and clinicians to ensure and promote the quality of information and to use information in decision making processes.

There are 5 key interlinked strands to the IG policy:

- · Openness
- · Legal compliance
- · Information security
- · Quality assurance
- · Records management

4. Openness

- ·Non confidential information about the Practice and its services should be available to the public through a variety of media.
- 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 Freedom of Information policies and arrangements.
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients in line with the NHS Constitution.
- The Practice will have clear procedures and arrangements for liaison with the press and broadcasting media as indicated within the Media Handling Policy.

- The Practice will have clear procedures and arrangements for handling queries from patients and the public.

5. 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 duty of 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).

6. 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 undertake risk assessments to determine appropriate security controls are in place for existing or potential information systems
- The Practice will undertake risk assessments to determine appropriate security controls are in place for existing or potential information systems
- The Practice will promote effective confidentiality and security practice to its staff through policies, procedures, induction 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.
- The Practice will use BS ISO/IEC 27001: 2005, BS ISO/IEC 27002: 2005 BS 7799-2: 2005 as the basis of its information security management arrangements.

7. Information Quality Assurance

- The Practice will establish and maintain policies and procedures for information quality assurance.
- The Practice will undertake or commission annual assessments and audits of its information quality.
- Managers and clinicians 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 definitions of data items, in accordance with national standards.
- The Practice will promote information quality and effective records managements through policies, procedures, induction and training.

8. Records Management

- The Practice will establish and maintain policies and procedures for the effective management of records
- The Practice will undertake or commission annual assessments and audits of its records management
- Managers and clinicians are expected to ensure effective records management within their service areas

- The Practice will promote records management through policies, procedures and training
- The Practice will use Records Management: NHS Code of Practice as its standard for records management

9. Responsibilities

- It is the role of the Partners to define the Practice's policy in respect of IG, taking into account legal and NHS requirements. The Partners are also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.
- All information used in the NHS is subject to handling by individuals and it is necessary for these individuals to be clear about their responsibilities. The Practice must ensure: support and appropriate education and training are provided for all staff.
- To manage its obligations the Practice will issue and support standards, policies and procedures ensuring information is held, obtained, recorded, used and shared correctly.
- Lead Partner on Clinical Governance for the Practice has overall accountability for IG in the Practice and is required to provide assurance, through the Statement of Internal Control (SIC), that all risks relating to information are effectively managed.
- The Information Governance Sub Committee (IGSC) is responsible for overseeing day to day IG issues; ensuring the IG improvement plan is maintained and monitored against the requirements of the IG toolkit through the co-ordination of different workstreams; developing and maintaining policies, strategies, structures, procedures and guidance and raising awareness of information governance. The Committee will also ensure annual assessments and submissions of the toolkit are undertaken The IGSC is accountable to the Integrated Governance Committee.
- The Information Governance Manager is responsible for raising awareness throughout the Practice with regard to the requirements of the information governance toolkit, for ensuring mandatory standards are met and providing support to Practice staff and workstreams.
- All staff, whether permanent, temporary or contracted and contractors 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.

10. Training and Awareness

- IG training is a mandatory requirement of induction training. All new staff will receive instruction to complete e-learning modules within the IG toolkit e-learning programme. All staff are required to complete annual IG training via the IG toolkit e-learning programme.

11. Monitoring and Audit

- The Practice will monitor this policy and related strategies, policies and guidance using the self assessment of the Information Governance Toolkit requirements and standards.
- The IGSC will implement the information governance requirements and standards using action plans and regular updates.
- Annual reports and proposed actions and development plans will be presented to the Partners for approval.
- The Practice will monitor compliance with the core Care Quality Commissions standards relating to information governance.

12. Legal Framework

- There are a number of legal obligations placed upon the Practice for the use and security of personally identifiable information. There are requirements to appropriately disclose information when required. The main relevant legislations are:
    - Data Protection Act 1998

  - Human Rights Act 1998
  - Access to Health Records Act 1990
  - Computer Misuse Act 1990
  - Copyright, Designs and Patents Act 1988
  - 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 2001
  - Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice
  - Regulations 2000)
  - Public Interest Disclosure Act 1998
  - NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases)
  - Directions 2000
  - 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. Regulatory Framework

- In relation to many of the above the NHS has set out and mandated a number of elements of regulations that constitute “information governance” through a national programme.
- The DSP Toolkit issued initially in November 2003 requires the Practice to assess their progress against set standards and currently encompasses the following initiatives or work areas:
  - Information Governance Management
  - Confidentiality and Data Protection Assurance
  - Information Security Assurance
  - Clinical Information Assurance
  - Secondary Use Assurance
  - Corporate Information Assurance
- The toolkit continues to develop and the focus within this section will need significant periodical review.
- The Caldicott Guardian Manual 2010, based upon a report by Dame Caldicott in 1997, for the audit and improvement of the use of patient identifiable data. ISO/IEC 27001: 2005, BS ISO/IEC 27002: 2005 BS 7799-2: 2005 is the Standard for Information Security Management which was originally mandated for the NHS in 2001.
- Information Quality Assurance
- Confidentiality: NHS Code of Practice November 2003
- NHS Guidance on Consent to Treatment
- Records Management: NHS Code of Practice March 2006 replacing HSC 1999/053 For the Record.
- Healthcare Commission Annual Health Check.

14. Policy Implementation

- This policy will be implemented through the DSP Toolkit assessment and action plan which will revise and develop the IG Policy along with associated procedures.
- The Practice will also work with Cornwall Information Technology Services (CITS) and Cornwall Kernow CCG to implement this policy.