East Staffordshire Clinical Commissioning Group

Information Governance Strategy

Ratified by:	CCC Governing Body
Date ratified:	28th February 2013
Name of originator / author:	Hayley Gidman, Senior Information Governance & Information Security Manager – NHS Staffordshire Commissioning Support Service
Name of responsible committee/individual:	QIPP Finance & Performance Committee David Harding (Chair)
Date issued:	28th February 2013
Review date:	31st March 2014
Date of first issue	28th February 2013
Target audience:	All Staff, including contractors and temps

CONSULTATION AND RATIFICATION SCHEDULE

Name and Title of Individual	Date Consulted
Wendy Kerr (CCG SIRO)	
David Harding (QF&P Chair)	

Name of Committee	**Date of Committee**
QIPP Finance & Performance	27th Feb 2013
CCG Governing Body	28th Feb 2013

VERSION CONTROL

Policy Name: Information Governance Policy			
Version	**Valid From**	**Valid To**	**Document Path/Name**
1.0	**Feb-2013**	**Mar-2014**	**ESCCG IG Strategy.doc**

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 throughout the Clinical Commissioning Group (CCG). It plays a key part in Clinical Governance, service planning and performance management.

It is therefore of paramount importance that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for Information Management. This is so as to assure and demonstrate the proactive use of information as determined by legislative acts, statutes, regulatory requirements and best practice.

Information Governance is a "*framework for handling information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service"*. It brings together within a singular cohesive framework, the interdependent requirements and standards of practice.

Information Governance (IG) combines Information Security, Corporate Governance and Business Continuity, and the increasing legislative and regulatory requirements, into a single, unified management framework.

Information Governance is not simply a matter of good corporate housekeeping. Good Information Governance can undoubtedly lead to efficiency gains and make for more effective management.

The Trust is required to have effective arrangements in place to govern the uses of information and information systems, as set out in the Information Governance Toolkit, Care Quality Commission – Essential Standards of Quality and Safety, and the NHS Litigation Authority Risk Management Standards.

2. Purpose

This Strategy sets out the approach to be taken within the CCG to ensure legal and regulatory compliance for the management of information.

The Information Governance Strategy cannot be seen in isolation, as information plays a key part in Corporate Governance, strategic risk, Clinical Governance, service planning, informatics, performance and business management. This Strategy therefore is closely linked with other CCG strategies to ensure integration with all aspects of our business activities.

3. Scope

The principles cover all aspects of information handling within the CCG, including patient / service user information, staff-related information and CCG information. The principles cover all aspects of handling information, including structured record systems (paper and electronic).

There are two key components underpinning this Strategy, which are:

- The CCGs Information Governance Policy, which outlines the objectives for Information Governance

- An annual action / improvement plan arising from a baseline assessment of the NHS (*Connecting for Health*) Information Governance Toolkit standards, within the following initiative areas:

  - Information Governance Management
  - Confidentiality and Data Protection
  - Information Security Assurance
  - Clinical Information Assurance
  - Secondary Use Assurance
  - Corporate Information Assurance

The Information Governance agenda encompasses the following areas:

- ✓ Caldicott
- ✓ NHS Confidentiality Code of Practice
- ✓ Data Protection Act (1998)
- ✓ Freedom of Information Act (2000)
- ✓ Records Management (Health, Business and Corporate)
- ✓ Information Security
- ✓ Information Quality
- ✓ Confidentiality
- ✓ Openness
- ✓ Legal Compliance

'In the event of an infection outbreak, flu pandemic or major incident, the CCG *recognises that it may not be possible to adhere to all aspects of this document. In such circumstances, staff should take advice from their manager and all possible action must be taken to maintain ongoing patient and staff safety'*

4. Duties & Responsibilities

- **The QIPP, Finance & Performance Committee**

Information Governance requires clear lines of accountability for policy, practice and implementation. The QIPP, Finance & Performance (QF&P) Committee, in conjunction with the Chief Finance Officer (CFO) and Head of Performance & Governance, will ensure coherence, clarity and consistency in the way information is governed within the CCG.

The QF&P Committee is accountable to the CCG's Governing Body. The Committee has overall responsibility for overseeing the implementation of this Strategy, the Information Governance Policy and the Information Governance Action Plan.

All are subject to periodic review and the reporting of progress on these will be via the QF&P Committee and CCG Governing Body. There is clinical and corporate representation on the Committee to ensure that Information Governance is embedded within the organisational structure.

- **Information Governance Lead (based within the Staffordshire Commissioning Support Service)**

  The Information Governance Lead is responsible for:

  - ✓ Co-ordinating all Information Governance initiatives and producing the annual improvement plan / work programme;
  - ✓ Providing operational support including training, query resolution, incident support and legal compliance requirements, e.g. Data Protection Act (1998) and Freedom of Information Act (2000) compliance;
  - ✓ Routine performance reporting to the Governance and Quality Committee and to Trust Board

- **Managers**

  Managers have a responsibility to ensure that all CCG Direct Reports are aware of the Information Governance Strategy and associated policies.

- **All Staff**

  All CCG staff will be held responsible for maintaining compliance with legal, statutory and organisational Information Governance requirements.

5. Process

- **Aims**

  Information Governance has four fundamental aims:

(a) *To support the provision of high quality care by promoting the effective and appropriate use of information;*

(b) *To encourage responsible staff to work closely together, preventing duplication of effort and enabling efficient use of resources;*

(c) *To develop support arrangements and provide staff with appropriate tools and support to enable them to carry out their responsibilities to consistently high standards;*

(d) *To enable the CCG to understand performance and manage improvement in a systematic and effective manner.*

The aim of this Strategy is to ensure the effective management of Information Governance by:

- Complying with all legislation;
- Establishing, implementing and maintaining policies for the effective management of information;

- Ensuring a consistent approach within the NHS with regard to information management;
- Recognising the need for an appropriate balance between openness and confidentiality in the management and use of information;
- Ensuring all CCG staff follow and promote best practice;
- Ensuring maintenance or year on year improvement with the Information Governance Toolkit assessment;
- Developing an Information Governance culture throughout the CCG;
- Helping staff to manage personal information for the benefit of patient care;
- Reducing duplication and looking at new ways of working effectively and efficiently;
- Minimising the risk of breaches of personal data;
- Minimising inappropriate uses of personal data.

Strategy Implementation

Strategic Goal	Objective	Action	Responsible Director	Lead Person	Target Date
Responsibility and Accountability *To provide a clear system of accountability and responsibility for Information Governance*	To have adequate governance in place to support the current and evolving Information Governance agenda	Establish clear lines of management and accountability for Information Governance, including setting up a forum for handling IG issues [to include senior managers and representatives from across the CCG]	CFO	Head of Performance & Governance	1st April 2013
	To develop / implement confidentiality and data protection assurance	The Caldicott Framework will be implemented to ensure that all staff members are aware of their individual responsibility regarding data protection and confidentiality issues and are also aware of how the work are links with the broader Information Governance Agenda.	CFO + Chief Nurse	Head of Performance & Governance	1st April 2013
	To develop and implement Information Quality and Records Management	To ensure that responsibility is allocated appropriately throughout the CCG and that these responsibilities are formalised in all relevant job descriptions.	CFO	Head of Performance & Governance	1st April 2013
	To develop and implement information security (IS) management, and support the identification of controls	All staff should have clearly defined IS responsibilities, with lead responsibility assigned in a transparent manner. The lead should be effectively trained and able to co-ordinate staff in meeting their responsibilities. This will be facilitated by the implementation of the SIRO Framework and full utilisation of the Information Security Management System.	CFO	Head of Performance & Governance	1st April 2013
	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disruption to its Information Assets; and to ensure their timely resumption should an event occur	Business Continuity planning is a core component of corporate risk management and emergency planning. Its purpose is to counteract serious interruptions to a CCG's business activities.	CFO	Head of Performance & Governance	1st April 2013

Strategic Goal	Objective	Action	Responsible Director	Lead Person	Target Date
	To develop and implement an Information Lifecycle Management (ILM) Policy	The CCG should have in place a CCG-wide ILM policy, which includes the process for managing risks associated with clinical records in all media. A strategy for implementing the policy should also be in place, identifying the resources needed to ensure records of all type are properly controlled, tracked, accessible and available for use and for eventually archiving or otherwise disposing of records.	CFO	Head of Performance & Governance	1st September 2013
	To comply with corporate IG responsibilities for participation in NHS *Connecting For Health* (CFH) provided infrastructure and services	CFH has implemented a Statement of Compliance (SoC), containing corporate standards that govern connection to / use of CFH-provided infrastructure and national services. CCGs are required to provide this before CFH services are provided.	CFO	Head of Performance & Governance	1st April 2013
	To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements	The CCG will only be able to comply with these duties where it has ensured that third parties with whom it contracts are subject to / comply with patient confidentiality, information security and data protection requirements.	CFO	Head of Performance & Governance	1st April 2013
	To develop and implement staff induction procedures effectively that raises the awareness of Information Governance	To maintain its information handling standards, the CCG must ensure that all new staff are provided with clear guidelines on their own obligations for confidentiality, data protection and information security.	CFO	Head of Performance & Governance	1st April 2013
	To develop and implement a confidentiality code of conduct that provides staff with clear guidance on the disclosure of patient personal information.	All organisations have a legal duty to keep patient information confidential and secure. The provision of guidance to staff regarding individual responsibility for safeguarding / preserving confidentiality and security will assist the CCG to ensure this duty is met.	CFO	Head of Performance & Governance	1st April 2013

Strategic Goal	Objective	Action	Responsible Director	Lead Person	Target Date
Security *To provide guidance that maintains appropriate confidentiality, security and integrity for information governance.*	To have a formal information security risk assessment and management programme that is adequately documented, implemented and regularly reviewed	A methodical information security risk assessment / management process will be in place to ensure that the CCG identifies, implements and manages controls to monitor / reduce the risk to the CCG, its patient-identifiable information and other critical information assets.	CFO	Head of Performance & Governance	1st April 2013
	To achieve and maintain appropriate protection of all CCG information assets	All information assets should be identified and have a nominated Information Asset Owner (IAO) to ensure appropriate protection is maintained. The SIRO should ensure IAOs are identified for all assets and responsibility for managing risks assigned. Whilst responsibility for implementing and managing information assets controls may be delegated to IAAs, accountability should remain with the nominated owner of the asset.	CFO	All CCG IAOs & IAAs	1st April 2013
	To prevent loss, damage, theft or compromise of information assets and interruption to the CCG's activities	Protection of equipment (including off-site) is necessary to reduce the risk of unauthorised access to data and to protect against loss or damage of information assets. Consideration should also be given to equipment siting and disposal. Special controls may be required to protect against physical threats, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.	CFO	All CCG IAOs & IAAs	1st April 2013
	To ensure that information security is a fundamental consideration for local Information Asset design and operation	For best effect, information security requirements should be identified and agreed prior to the design, development and/or implementation of an information asset as part of its IG accreditation documentation set. Responsibilities and procedures for the management / operation of all information assets should be defined and agreed.	CFO	All CCG IAOs & IAAs	1st April 2013

Strategic Goal	Objective	Action	Responsible Director	Lead Person	Target Date
Access *Information governance will promote the awareness of legislation and provide a consistent approach for employees and others who have a legitimate right of access to CCG information, and ensure compliance with Access to Health Records, Data Protection and Freedom of Information legislation.*	To effectively control access to information assets	Access to assets, processing facilities and business processes should be controlled on the basis of business need / security policy requirements. Access control rules should take account of both local and national policies for information dissemination and authorisation.	CFO	All CCG IAOs & IAAs	1st April 2013
	To have defined, documented and agreed access rights for all users of CCG-based information systems and services	Formal procedures are in place to control the allocation of access rights to local systems / services. These should cover all stages in the lifecycle of user access, from initial registration of new users to final de-registration of users no longer requiring access. Special attention should be given, where appropriate, to the need to manage the allocation of privileged access rights, which may allow support staff to override system controls.	CFO	All CCG IAOs & IAAs	1st April 2013
	To ensure the protection of information communicated over local networks and for the protection of the supporting infrastructure, including wireless networks	The secure management of networks (spanning CCG boundaries + beyond), requires careful consideration to dataflow, legal implications, monitoring and protection. Additional controls may also be required to protect sensitive information passing over public networks.	CFO	All CCG IAOs & IAAs	1st April 2013
Audit *To audit and measure the implementation of the information governance strategy against agreed standards.*	To ensure that the CCG is able to identify and retrieve information when and where it is needed	The CCG must have procedures for creating, filing and tracking / tracing paper or electronic records that supports efficient location and retrieval in accordance with the Records Management: NHS Code of Practice	CFO	All CCG IAOs & IAAs	1st April 2013
	To establish what records are held, where they are located and the form in which they are held	Good records management practice requires that the CCG undertakes an audit of practice and systems. The audit will assist the CCG to comply with legal provisions, such as the Freedom of Information Act 2000.	CFO	All CCG IAOs & IAAs	1st April 2013

Strategic Goal	Objective	Action	Responsible Director	Lead Person	Target Date
Training *To provide training and guidance on legal and ethical responsibilities and operational good practice for all staff involved in information governance.*	To ensure that key messages about Information Governance requirements should be included in induction procedures	To maintain information handling standards throughout the CCG, all new staff must be provided with clear guidelines on their own obligations for confidentiality, data protection and information security.	CFO	Head of Performance & Governance	1st April 2013
	To ensure that the CCG provides Information Governance training to key staff based upon training needs assessments	The CCG should routinely assess IG training needs and evaluate the training undertaken. The CCG should work towards providing IG training at a level comparable to health + safety training provision.	CFO	Head of Performance & Governance	Annual
	To ensure that CCG staff are aware of a patient's right to restrict disclosure of their personal information	Staff must ensure that as far as possible, the patient's right is adhered to / respected; and that they are aware of the possible disciplinary sanctions for a failure to respect these. Guidance for staff will be included in the confidentiality code of conduct.	CFO	Head of Performance & Governance	1st April 2013
Patient Knowledge	To ensure that patients are asked before their personal information is used in ways that do not directly contribute to or support the delivery of their care; and that patients' decisions to restrict the disclosure of information are appropriately respected	To meet the legal requirements of the Data Protection Act and the common law, the CCG should ensure that it has procedures in place to gain specific informed consent to use that information for a secondary purpose.	CFO	Head of Performance & Governance	1st April 2013
	To ensure that patients are informed about the proposed uses of their personal information and the importance of providing accurate information to NHS staff	Communication materials should clearly and concisely inform about confidentiality, and the way that information is used and shared. This will be supported by an active policy to ensure that patients are fully informed of the ways in which personal information is used, and in particular, when it is to be used for a purpose not originally envisaged when first collected.	CFO	Head of Performance & Governance	1st April 2013