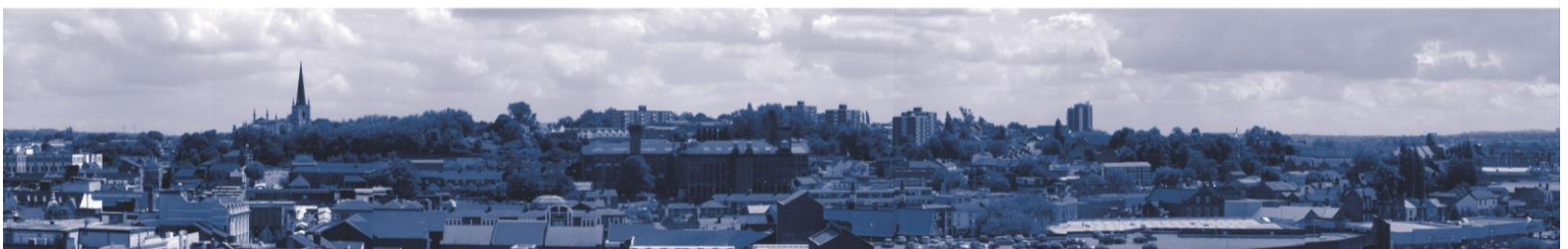
NHS

Walsall Clinical Commissioning Group

Information Governance Policy

Walsall Clinical Commissioning Group

WCCG



Information Governance Policy
For
Walsall Clinical Commissioning Group

The Audit and Governance Committee approved this document on:

Date: 17 September 2018
Signed: Chair of the committee
Signed: Designated Senior Officer

Please note that the Intranet version of this document is the only version that is maintained. Any printed versions should therefore be viewed as 'uncontrolled' and may not be the most up-to-date.

Version:	V4.0
Status	Ratified
CCG Lead	Sara Saville, Head of Corporate Governance
Senior Officer responsible	Chief Officer, Simon Brake
Ratified by:	Audit & Governance Committee
Date ratified:	17 September 2018
Date Policy is Effective From	Ratification date
Expiry date:	March 2019
Review date:	February 2019
Date of Equality and Diversity Impact Assessment	
Date of Health Inequalities Impact Assessment	
Target audience:	CCG staff Consultants Bank and agency staff Third party contractors Volunteers Temporary staff Any individuals 'using' CCG information Any individuals receiving information on behalf of the CCG
National Documents	- Data Protection Act 2018 - General Data Protection Regulation (GDPR)Human Rights Act 1998 - Freedom of Information 2000 - Access to Health Records Act 1990 (where not superseded by the Data Protection Act) - Computer Misuse Act - Copyright, designs and patents Act 1988 (as amended by the -Copyright Computer programs regulations 1992 - Crime and Disorder Act - Electronic Communications Act 2000 - Regulation of Investigatory Powers Act 2000 - Common Law Duty of Confidentiality - National Health Service Act 1977
CCG linked documents	- Confidentiality Code of Conduct - Data Protection Policy - Freedom of Information Policy - Destruction and Retention schedule for records - Information Security Policy - Email Policy and Code of Conduct - Internet Use Policy - Safe Haven Policy - Subject Access Request Procedure - Pseudonymisation Policy

Distribution of the document	Hard copies available at reception, accessible from Website, IG team and IG Newsletter.
Implementation of the document	December 2012
Document Control and Archiving	Obsolete or superseded documents will be removed from the intranet and where relevant replaced with an updated version. Previous versions will be archived in the safeguard system in accordance with the Records Management NHS Code of Practice; disposal and retention schedule.
Monitoring Compliance and Effectiveness	This policy will be monitored through the regular assurance reports to Safety Quality and Performance Committee.
References	

CONTRIBUTION LIST
Key individuals involved in developing the document

Name	Designation
Dr R Mohan	Governing Body Member Caldicott Guardian (v2.0)
Dr N Asghar	Governing Body Member IT lead (v2.0)
Kevin McGovern	Head of Finance – Information (v 2.0)
Sally Roberts	Director of Governance Quality & Safety
Sara Saville	Head of Corporate Governance
Serena Causer	Corporate Governance Officer

Circulated to the following for consultation

Name/Committee/Group/	Designation
SQP	
IG Function Leads	
Audit & Governance Committee (A&G)	

Comments received from consultation

Name/Committee/Group	Comments
Governing Body	*Could we include emergency action on breeches if they are detrimental* – this is covered in the SI policy
Medicines management	*As part of our responsibilities on what information we are required to make available perhaps worth noting that there are national directives which will impact on the CCG, .e.g the need to publish information to ensure that NICE TAGs are included within local formularies* –this is covered in the openness section
Commissioning	*should there be anything on potential conflict of interest* – this is covered in the CCG constitution

Version Control Summary

Significant or Substantive Changes from Previous Version

Version	Date	Comments on Changes	Author
	2010	NHSW Information Governance Policy	Kirstie McMillan
V1.1	2012	WCCG Information Governance Policy consultation	Sara Saville
V 2.0	2012	WCCG Information Governance Policy ratified	Sara Saville
V2.1	May 2018	Reflect General Data Protection Regulation and Data Protection Officer role	Serena Ellis
V4.2	August 2018	Reflect Data Protection Act 2018 and General Data Protection Regulation	Serena Ellis

Contents

1.0 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.

2.0 Principles

This policy covers all aspects of information within the organisation including:

1. patient/client/service user
2. personnel
3. organisational

It covers all aspects of handling information including:

1. structured record systems paper and electronic
2. transmission of information – fax, email, post and telephone

The CCG recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The CCG 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 CCG 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. Any sharing must be done lawfully within the Organisation's Information Sharing Protocols.

The CCG 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 four key interlinked strands to the information governance policy:

1. Openness
2. Legal compliance
3. Information security
4. Quality assurance

2.1 Openness

1. Non-confidential information on the CCG and its services should be available to the public through a variety of media, in line with the CCG's value of transparency.
2. Risk assessment will be in line with the Risk Management Strategy and Risk Management Plan to determine appropriate and effective information governance controls are in place.
3. The CCG will undertake or commission annual assessments and audits of its policies and arrangements for openness. Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.
4. 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 Organisation's Subject Access Request procedures.
5. The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media
6. The CCG will have clear procedures and arrangements for handling queries from patients and the public
7. Compliance with legal and regulatory framework will be achieved, monitored and maintained through the Data Security Protection Toolkit and associated procedures.

2.2 Legal Compliance

1. The CCG regards all identifiable personal information relating to patients as confidential except where national policy on accountability and openness requires otherwise.
2. The CCG will undertake or commission annual assessments and audits of its compliance with legal requirements
3. The CCG regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise
4. The CCG will establish and maintain policies to ensure compliance with the Data Protection Act 2018, General Data Protection Regulation, Human Rights Act and the common law confidentiality
5. The CCG 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)

2.3 Information Security

1. The CCG will establish and maintain policies for the effective and secure management of its information assets and resources
2. The CCG will undertake or commission annual assessments and audits of its information and IT security arrangements

3. The CCG will promote effective confidentiality and security practice to its staff through policies, procedures and training
4. The CCG will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
5. Information that is to be transferred for purposes other than direct patient care should not identify one person (unless identifiable information is necessary). The information should be in line with pseudonymisation, where the personal information is de-identified. The depersonalisation of the information increases the security of the individual.
6. For secondary uses, as defined within the Organisation's Pseudonymisation Policy, identifiable data must not be used. Instead staff should have access to pseudonymised data. Limited staff will have access to the identifiable raw data; however permission must be granted to ensure that personally identifiable data is required for the purpose and a record kept.

2.4 Information Quality Assurance

1. The CCG will establish and maintain policies and procedures for information quality assurance and the effective management of records
2. The CCG will undertake or commission annual assessments and audits of its information quality and records management arrangements
3. Managers and information Asset Owners will take ownership of, and seek to improve, the quality of information within their services. Regular reports must be sent to the Organisation's Senior Information Risk Officer (SIRO) including risk assessments of the information asset.
4. Wherever possible, information quality should be assured at the point of collection
5. Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
6. The CCG will promote information quality and effective records management through policies, procedures/user manuals and training

3.0 Responsibilities

It is the role of the Governing Body to define the CCG's policy in respect of Information Governance, taking into account legal and NHS requirements. The Governing Body is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

The Chief Officer is the lead on the Governing Body for Information Governance.

The Audit and Governance (A&G) Committee is accountable to the Governing Body for the assuring the compliance with information governance practices across the organisation and for the development of best practices including the integration of information governance with the rest of the work place and practice.

The A&G committee's responsibility will include the following:

- Recommending for approval related policies and procedures.
- Recommending for approval the annual submission of the compliance requirements in the Data Security Protection Toolkit and related action plan for improvement.
- To co-ordinate and monitor the Information Governance Strategy across the CCG.
- To carry out audits to ensure compliance of statutory and legal requirements.
- To report by exception to the Governing Body any information governance risks and concerns.

The IG Manger attends the A&G committee; the Chair of A&G represents the Governing Body with regular assurance reports on the activity of A&G. Any escalation of IG risks or issues can be taken through this route or if a more timely response is required through the Senior Management Team which includes the clinical lead sand senior managers in its membership.

The Data Protection Officer has overall responsibility for due diligence, data protection impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the GDPR and our own internal objectives and obligations.

The operational Information Governance lead is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the CCG and raising awareness of Information Governance.

Managers within the Trust are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

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.

4.0 Training

To ensure organisational compliance with the law and central guidelines relating to IG, staff must receive appropriate training. WCCG therefore have made IG training mandatory for all staff. WCCG aim to ensure that all staff should receive annual basic IG training appropriate to their role through online training through ESR.

All new staff will receive an in-house induction session. This will include the required IG awareness that all staff complete on an annual basis. It is the responsibility of the manager to ensure that the new staff member successfully completes the training.

Appointing Managers will be responsible for making new staff aware of the corporate policies including IG and where they can be accessed.