INFORMATION GOVERNANCE POLICY

Document Type	Corporate Policy
Unique Identifier	IG-004
Document Purpose	This policy provides assurance that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible high quality patient care
Document Author	Rob Neill, Head of Information Governance
Target Audience	All Worcestershire Health and Care NHS Trust staff
Responsible Group	Worcestershire Health and Care NHS Trust Quality and Safety Committee
Date Ratified	29 July 2016
Expiry Date	28 July 2019
Equality Impact Assessment	This Policy has been screened using the Equality Duty Assessment Form and does not require a full Equality Impact Assessment

This validity of this policy is only assured when viewed via the Worcestershire Health and Care NHS Trust website (hacw.nhs.uk.) If this document is printed into hard copy or saved to another location, its validity must be checked against the unique identifier number on the internet version. The internet version is the definitive version.

If you would like this document in other languages or formats (i.e. large print), please contact the Communications Team on 01905 760020 or email communications@hacw.nhs.uk

Version History

Version	Circulation Date	Job Title of Person/Name of Group circulated to	Brief Summary of Change
0.1, 0.2, 1.0, 2.0, 3.0	07/09/2011	Information Governance Steering Group	See previous versions for comments. Held in M:\HACW\CompanySecretary\Information Governance\IG Policies
4.0	10/03/2014	Information Governance Steering Group	Include reference to *Prevent Strategy*
5.0	02/12/2014	Information Governance Steering Group	Update IG Management Framework in line with the latest version of IGT
	21/08/2015	Clinical Governance Sub-Committee	Update IG Management Framework in line with the latest version of IGT
6.0	29/07/2016	Information Governance Steering Group	Update IG Management Framework in line with the latest version of IGT
			Reviewed and aligned with the latest Department of Health guidelines.

Accessibility

- Interpreting and Translation services are provided for Worcestershire Health and Care NHS Trust, including:
- Face to face interpreting;
- Instant telephone interpreting;
- Document translation; and
- British Sign Language interpreting

Please refer to intranet page: http://nww.hacw.nhs.uk/a-z/services/translation-services/ for full details of the service, how to book and associated costs.

Training and Development

Worcestershire Health and Care NHS Trust recognises the importance of ensuring that its workforce has every opportunity to access relevant training. The Trust is committed to the provision of training and development opportunities that are in support of service needs and meet responsibilities for the provision of mandatory and statutory training.
All staff employed by the Trust are required to attend the mandatory and statutory training that is relevant to their role and to ensure they meet their own continuous professional development.

Co-production

Co-production reflects the values of the NHS Constitution which promotes the full involvement of patients, staff, families, carers and professionals inside and outside the NHS. The Trust expects that all healthcare professionals will provide clinical care in line with best practice. In offering and delivering that care, healthcare professionals are expected to respect the individual needs, views and wishes of the patients they care for, and recognise and work with the essential knowledge that patients bring. Staff will demonstrate a respect for patient diversity and a capacity to respond with flexibility. As facilitators of care, staff will work with patients and carers to help them understand their diagnosis and treatment options. Staff bring knowledge and expertise to enable and empower patient partners to make the right choices for themselves.

Contents

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, performance and business management.

It is therefore of paramount importance to ensure that information is effectively and securely managed and that appropriate policies, procedures and management accountability and structures are in place to provide a robust framework for information governance.

Worcestershire Health and Care NHS Trust (The Trust) will establish and maintain policies and procedures to ensure compliance with relevant legislation, such as the Data Protection Act 1998, and the requirements contained in the Department of Health's Information Governance Toolkit.

This policy gives assurance to the Trust, service users and the Care Quality Commission that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible high quality patient care.

2. Purpose of document

- To support the provision of high quality care by promoting the effective and appropriate use of information

- To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources

- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards

- To enable the Trust to understand its own performance and manage improvement in a systematic and effective way

- To provide a robust Information Governance framework covering:

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

3. Scope

This policy covers all information assets within the Trust, including but not limited to:

- Patient/Client/Service User information

- Personnel information

- Organisational information

- Structured record systems – paper and electronic

- Transmission of information – fax, email, post and telephone

This policy covers all information systems purchased, developed and managed by/or on behalf of the Trust and any individual directly employed or otherwise by the Trust.

4.   Principles

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

The Trust 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 Trust 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 Trust 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 this Information Governance Policy:

- Openness and Transparency
- Legal Compliance
- Information Security
- Quality Assurance

Openness & Transparency

- The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

- Information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott and the regulations outlined in the Data Protection Act. Non-confidential information on the Trust and services will be available to the public through the Trust's website or requests under the Freedom of Information Act.

- Service users will have access to information relating to their own health care, options for treatment and their rights as patients. There will be clear procedures and arrangements for handling queries from patients and the public.

- The Trust 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 within set parameters relating to its importance via appropriate procedures and computer system resilience.

- The Trust regards all personal identifiable information relating to service users as confidential. Compliance with legal and regulatory frameworks will be achieved, monitored and maintained.

- The Trust regards all personal identifiable information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

Legal Compliance

- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements by means of the Department of Health's Information Governance Toolkit.

- The Trust will establish and maintain policies and procedures to ensure compliance with the Data Protection Act, Human Rights Act, Freedom of Information Act and the common law duty of confidentiality.

- The Trust has established and will maintain policies for the controlled and appropriate sharing of patient information with other agencies.

- The Trust will maintain a comprehensive range of policies supporting the information governance framework.

- In line with the *Prevent Strategy*, the Trust will ensure that data collected about persons - staff or service-users - for the purposes of preventing or detecting radicalisation will be necessary and proportionate. There should be transparency about the way it is collected and the purpose for which it is intended. The data must be protected and shared securely as set out in Information Sharing Agreements between the Trust and local partners and those procedures must be transparent.

Information Security

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources.

- The Trust will undertake or commission annual assessments and audits of its information security arrangements.

- The Trust will promote effective confidentiality and information security practices to its staff through policies, procedures and mandatory training.

- The Trust will establish and maintain information governance related incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

Information Quality Assurance

- The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records.

- The Trust 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 Trust will promote information quality and effective records management through policies, procedures/user manuals and training.

5. Responsibilities and duties

Trust Board

The Trust Board is responsible for defining the Trust's policy in respect of information governance, taking into account legal and NHS requirements.

The Trust Board will be informed and assured that the Trust is meeting all national and local information governance objectives via reports to the Worcestershire Health and Care NHS Trust Quality and Safety Committee. The Trust Board will also be informed and assured directly by the Trust's Information Governance Lead Director.

The Trust Board is responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

The Trust Board shall be informed by the Information Governance Lead Director of any local or national information governance issues that may affect this policy.

Chief Executive

The Chief Executive as Accountable Officer has overall accountability and responsibility for information governance in the Trust and is required to provide assurance, through the Statement of Internal Control that all risks to the Trust, including those relating to information governance, are effectively managed and mitigated.

The Chief Executive has delegated responsibility for information governance to the Information Governance Lead Director.

The Senior Information Risk Owner (SIRO)

Senior level ownership of information risk is a key factor in successfully raising the profile of information risks and to embedding information risk management into the overall risk management culture of the Trust. Senior leadership through the appointment of the Director of Finance to the role of Senior Information Risk Owners (SIRO) demonstrates the importance of ensuring information governance remains high on the Trust Board agenda.

The SIRO is expected to understand how the strategic business goals of the Trust may be impacted by information risks. The SIRO will act as an advocate for information risk on the Trust Board and will provide written advice to the Accounting Officers on the content of its annual Statement of Internal Control in regard to information risk.

The SIRO will undertake strategic information risk management training at least annually.

The SIRO will ensure the maintenance of a risk assessed information asset register. Each information asset will have an Information Asset Owner and an Information Asset Administrator.

The SIRO will provide an essential role in ensuring that identified information threats are followed up and incidents managed. They will also ensure that the Trust Board and the Accountable Officer is kept up to date on all information risk issues. The role will be supported by the Caldicott Guardian, the Information Governance Lead Director and the Head of Information Governance.

The Caldicott Guardian

The Caldicott Guardian is the senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. They play a key role in ensuring that the Trust satisfies the highest practicable standards for handling patient identifiable information.

The Caldicott Guardian acts as the 'conscience' of the Trust and actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information.

The Caldicott Guardian also has a strategic role, which involves representing and championing information governance requirements and issues at Trust Board and Senior Management Team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

The Caldicott Guardian for Worcestershire Health and Care NHS Trust is the Medical Director.

The Head of Information Governance is the Delegated Authority for the Caldicott Guardian.

Caldicott issues are discussed at the Trust's Records Management Steering Group as a standing agenda item and as part of the overall Caldicott function.

Information Governance Lead Director

The Company Secretary has been delegated responsibility for information governance by the Chief Executive for Worcestershire Health and Care NHS Trust.

The Information Governance Lead Director shall ensure that a framework is in place so that the information governance agenda is appropriately resourced and that staff are adequately skilled and experienced.

The Information Governance Lead Director shall ensure that the necessary information governance reporting and monitoring procedures are in place.

The Head of Information Governance

The Head of Information Governance has been assigned responsibility for information governance by the Information Governance Lead Director.

The Head of Information Governance is responsible for overseeing day to day information governance issues; developing and maintaining policies, standards, procedures and guidance.

Directors, Associate Directors, Service Delivery Unit Leads, Senior Managers and Team Managers

All Managers within the Trust are responsible for ensuring that the policy and supporting standards and guidelines are built into local processes to ensure on-going compliance.

Individual members of staff

All staff should ensure that they are aware of their own personal responsibilities with regard to information governance and should make sure that they comply with these on a day to day basis.

Other

Computacenter provide Information Security advice and support for the Trust.

6. Groups and committees

The Information Governance Steering Group will ensure that there are effective policies and management arrangements covering all aspects of information governance, in line with this policy.

The Information Governance Steering Group is responsible for raising awareness and coordinating information governance across the Trust.

The Information Governance Steering Group will assist in promoting mandatory training and is responsible for implementing relevant guidance to all employees to protect the confidentiality and security of personal and corporate information.

The Information Governance Steering Group receives its authority from, and has overall accountability to the Worcestershire Health and Care NHS Trust Clinical Governance Sub-Committee. Outstanding issues will be reported to this Committee.

7.   Monitoring implementation

The Trust will monitor this policy through the Information Governance Steering Group and continued compliance with the Department of Health's Information Governance Toolkit requirements.

The Trust will undertake an annual Information Governance self-assessment using the latest version of the Department of Health's Information Governance Toolkit.

The final Information Governance Toolkit submission assessment score reported by the Trust is used by the Care Quality Commission to risk assess Outcome 21 - records (and other standards as appropriate) of Essential standards of quality and safety.

The Information Governance Steering Group will implement an annual Information Governance Action Plan.

Six monthly reports and proposed action/development plans will be presented to the Worcestershire Health and Care NHS Trust Clinical Governance Sub-Committee.

The Information Governance Lead Director will update the Senior Management Team on progress, development and performance of information governance in the Trust.

This policy will be reviewed every three years, or earlier if appropriate, to take into account any changes to legislation that may occur, and/or guidance from the Department of Health, the NHS Chief Executive and/or the Information Commissioners Office.

Staff will be advised of this policy through 'Team Brief'. The policy will be available to all staff via the Trust's website.

8.   Associated Trust Documentation

- Code of Conduct for Employees in Respect of Confidentiality
- Freedom of Information Policy
- Records Management Policy
- Information Governance leaflets on Data Protection
- IG Training Programme
- Information Security Policy
- Internet and Email Access Policy

9.   Related Legislation and NHS Guidance

- Data Protection Act 1998
- Access to Health Records 1990
- Human Rights Act 1998

- Freedom of Information Act 2000

- Regulation of Investigatory Powers Act 2000

- Crime and Disorder Act 1998

- Computer Misuse Act 1990

- Criminal Justice Act 2003

- Common Law Duty of Confidentiality

- Confidentiality: NHS Code of Practice

- NHS Care Record Guarantee for England

- International Information Security Standard: ISO/IEC 27002:2005

- Information Security: NHS Code of Practice

- Records Management: NHS Code of Practice

- Caldicott Principles

10.   Appendix 1: IG Management Framework

Information Governance Management Framework
Heading	**Requirement**	**Notes** All policies are available via the IG pages on the Trust website (http://nww.hacw.nhs.uk/a-z/services/information-governance)
Senior Roles	• IG Lead(s) • Senior Information Risk Owner (SIRO) **(see Requirement 14-307)** • Caldicott Guardian **(see Requirement 14-200)**	• Company Secretary (Gill Harrad), Head of IG (Rob Neill) • SIRO is the Director of Finance (Robert Mackie) • Caldicott Guardian is the Medical Director (Dr Andy Sant) • Records Manager (Maureen Bottrell) Other IG roles and responsibilities are detailed in the IG Policy, IG Mgt Framework and the IG Steering Group Terms of Reference
Key Policies **(see Requirement 14-105)**	• Over-arching IG Policy • Data Protection Act 1998/Confidentiality Policy • Organisation Security Policy • Information Lifecycle Management Policy • Corporate Governance Policy	• Information Governance Policy (approved by IG Group July 2016) • Data Protection Policy (approved by IG Group Dec 2015) • Code of Conduct for Employees in Respect of Confidentiality (approved by IG Group July 2016) • Information Security Policy and other associated information security policies (approval dates in County IG Mgt Framework) • Records Management Policy (approved by IG Group Dec 2013) • Freedom of Information Policy (approved by IG Group Dec 2014)
Key Governance Bodies	IG Board/Forum/Steering Group	• Trust IG Steering Group • Countywide IG Steering Group
Resources	Details of key staff roles and dedicated budgets	• IG Officer • IG Officer / RA Coordinator • RA Agent • FOI Officer • Info Security Manager function (Computacenter) • IG/RM budget held by Company Secretary
Governance Framework	Details of how responsibility and accountability for IG is cascaded through the organisation. **(see Requirements 14-200 & 14-307)**	• All staff contracts include IG clauses • Contractors Confidentiality Agreement v8.0 • Information Asset Owners, Information Asset Register etc – described in Information Risk Policy • Examples of 3rd Party Contracts e.g. Whitefoot Forward
Training & Guidance **(see Requirement 14-112)**	• Staff Code of Conduct **(see Requirements 14-201, 14-202 & 14-203)** • Training for all staff • Organisation Security Policy • Training for specialist IG roles	• Code of Conduct for Employees in Respect of Confidentiality • Information Governance Training is mandatory for all staff. Guidance is available on the intranet • IG Booklet, slides, DVD on Trust induction • Information Security Policy (approval date in County IG Mgt Framework) • Training needs analysis (TNA) for in Countywide Training Programme (approval date in County IG Mgt Framework)
Incident Management **(see Requirements 14-307, 14-301 & 14-302)**	Documented procedures and staff awareness	• Information Risk Policy (approved by IG Group Mar 2014) • Guidance for Reporting IG Related Incidents (approved by IG Group Sep 2013) • Links to Ulysses are included in Guidance • Links to Ulysses are on intranet