NHS
North Staffordshire
Combined Healthcare
NHS Trust

Doc level: Trustwide
Code ref: 7.08

Information Governance Policy

Lead executive	Director of Finance
Authors details	Health Records & Information Governance Manager

Type of document	Policy
Target audience	All Trust staff
Document purpose	This policy details how North Staffordshire Combined Healthcare NHS Trust will meet its national and legal responsibilities in the way that it handles its information and comply with all requirements for Information Governance (IG)

Approving meeting	Finance and Performance Committee/ Trust Board	Meeting date	8th November 2018
Ratification date	22nd November 2018	Review date	30th November 2021

Trust documents to be read in conjunction with	
Document code	Document name
4.18	Risk Management Policy
5.01	Incident Reporting Policy
7.01	Confidentiality of Patient and Employee Personal Information
7.02	Subject Access Request Policy
7.03	Information Security & Data Protection Policy
7.05	One Staffordshire Information Sharing Protocol

Document change history		Version	Date
What is different?	– This policy has been revised in line with legislation changes under the Data Protection legislation and changes made national to IG –		
Appendices / electronic forms	–		
What is the impact of change?	– Making all staff aware of changes in relation to IG – Ensuring that the Trust is compliant with its legal and national requirements in the way that information is handled.		

Training requirements	All staff are mandated to complete the online Data Security Awareness national training tool annually

Document consultation	
Directorates	
Corporate services	
External agencies	

Financial resource implications	No

External references
1. Data Protection Bill 2. General Data Protection Regulations (GDPR)

Monitoring compliance with the processes outlined within this document	Any breaches to this policy will be recorded within the Trust's incident reporting system and any breaches will be investigated accordingly.

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Less favourable / More favourable / Mixed impact**
Does this document affect one or more group(s) less or more favorably than another (see list)?		
– **Age** (e.g. consider impact on younger people/ older people)	No	
– **Disability** (remember to consider physical, mental and sensory impairments)	No	
– **Sex/Gender** (any particular M/F gender impact; also consider impact on those responsible for childcare)	No	
– **Gender identity and gender reassignment** (i.e. impact on people who identify as trans, non-binary or gender fluid)	No	
– **Race / ethnicity / ethnic communities / cultural groups** (include those with foreign language needs, including European countries, Roma/travelling communities)	No	
– **Pregnancy and maternity, including adoption** (i.e. impact during pregnancy and the 12 months after; including for both heterosexual and same sex couples)	No	
– **Sexual Orientation** (impact on people who identify as lesbian, gay or bi – whether stated as 'out' or not)	No	
– **Marriage and/or Civil Partnership** (including heterosexual and same sex marriage)	No	
– **Religion and/or Belief** (includes those with religion and /or belief and those with none)		
– **Other equality groups?** (may include groups like those living in poverty, sex workers, asylum seekers, people with substance misuse issues, prison and (ex) offending population, Roma/travelling communities, looked after children, local authority care leavers, and any other groups who may be disadvantaged in some way, who may or may not be part of the groups above equality	No	

groups)		
If you answered yes to any of the above, please provide details below, including evidence supporting differential experience or impact.		
Enter details here if applicable		
If you have identified potential negative impact: - Can this impact be avoided? - What alternatives are there to achieving the document without the impact? Can the impact be reduced by taking different action?		
Enter details here if applicable		
Do any differences identified above amount to discrimination and the potential for adverse impact in this policy?	No	
If YES could it still be justifiable e.g. on grounds of promoting equality of opportunity for one group? Or any other reason	N/A	
Enter details here if applicable		
Where an adverse, negative or potentially discriminatory impact on one or more equality groups has been identified above, a full EIA should be undertaken. Please refer this to the Diversity and Inclusion Lead, together with any suggestions as to the action required to avoid or reduce this impact. For advice in relation to any aspect of completing the EIA assessment, please contact the Diversity and Inclusion Lead at Diversity@northstaffs.nhs.uk		
Was a full impact assessment required?	No	
What is the level of impact?	Low	

CONTENTS

1. INTRODUCTION

1.1 Information is a vital asset; the Trust recognises the importance of reliable information both in terms of the clinical management of individual patients and the efficient management of services and resources. Information Governance plays a key part in supporting clinical governance, service planning and performance management. It is therefore of paramount importance to ensure that all information is efficiently and legally managed, and that appropriate policies, procedures, and management accountability provide a robust governance framework for information management as described in the Data Security and Protection Toolkit (DSP Toolkit).

1.2 IG compliance is supported by the key roles of Caldicott Guardian, Senior Information Risk Officer (SIRO), Data Protection Officer and Chief Information Officer, who are supported by the Information Governance Manager. However all staff have a duty of confidentiality and an important role to play in ensuring the Trust is compliant with IG.

1.3 IG compliance is also supported by the identification of Information Asset Owners, Administrators, Information Mapping and Information Asset Register through a process of risk management.

1.4 The focus and objective of IG is that, via corporate teamwork, there is systematic management of the range of interrelated initiatives and work streams with the aim of addressing limitations thus raising standards that underpin the provision of high quality healthcare. IG should lead to improvements in:

- Information handling/disclosure of information (both personal and corporate)
- Patient/Public confidence in the NHS
- Staff training and development
- Data Standards

1.5 Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service.

1.6 The web-based Data Security Protection Toolkit requires continual formal co-ordination and management as Trusts are required to complete and submit their self-assessments on an annual basis. Annual reports and proposed action/development plans will be presented to the Trust's Executive Team.

1.7 The DSP Toolkit requires the organisation to be compliant with assertions and (mandatory) evidence items.

1.8 A further requirement is to define and develop appropriate management arrangements, work streams and remedial action plans to fulfil organisational requirements and to address areas of weakness.

2 POLICY STATEMENT – AIMS AND OBJECTIVES

2.1 The Trust recognises, in the management of and use of all information, the need to facilitate, manage, and achieve an appropriate balance between openness and confidentiality. 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 personal information relating to patients and staff as well as 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.

2.2 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. The aim of this policy is to ensure that an appropriate IG structure is in place which adequately supports the Trust to manage all IG responsibilities.

3 SCOPE OF THE POLICY

3.1 The Information Governance policy and the required work streams have 4 key interlinked strands:

- **Openness within the NHS**
- **Legal Compliance and the NHS Confidentiality Code of Practice**
- **Information Security**
- **Information Quality Assurance/Data Quality**

3.2 The philosophy, aims and requirements of IG have resulted in the need for an IG policy.

3.3 All corporate, operational functions, process, procedures, or policies based on, or which reference the use of patient/person identifiable information or corporate information must comply with the principles and standards of IG and address the standards of the relevant work streams. Therefore, the principles mandated with this IG policy are central to many other Trust policies and development or review of such policies must occur within the IG framework and as such the content of this policy must be referenced and adhered to. An overview and examples of linkage are contained in Appendix 2.

3.4 Openness with the NHS

3.4.1 From 1995 the NHS has been required to comply with a Code of Openness however the philosophy of the code was legally formalised by the Freedom of Information Act 2000 (FOIA), which became fully operational from January 2005. The effects of the FOIA apply fully and retrospectively to all information until its point of disposal.

3.4.2 The FOIA aims to promote a culture of openness and accountability amongst public authorities by providing the public with the rights of access to the majority of information held, but not necessarily created by, a public authority. It is expected that these rights will facilitate better public understanding of how public authorities carry out

their duties, why they make the decisions that they do and how they spend public money.

3.4.3 North Staffordshire Combined Healthcare NHS Trust is committed to achieving the following FOIA and IG objectives:

- The Trust will have clear procedures and arrangements for handling queries from patients and the public;
- All staff are aware of the rights of patients and the public to access corporate information and actively offer support;
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients;
- Non-confidential information on the Trust and its services be available to the public through a variety of media;
- The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act;
- The Trust will undertake or commission annual assessments and audits of its policies and arrangements for openness;
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.

3.4.4 In order to assist and facilitate these objectives the Trust is committed to actively publishing a wide range of information and policies on the Trust web-site and via other methods.

3.5 Legal Compliance and the NHS Confidentiality Code of Practice

3.5.1 Current Data Protection legislation (DPA) is the law that protects personal information and its uses and provides a legal framework that mandates all actions relating to information which identifies (living) individuals. The NHS Confidentiality Code of Practice (COP) underpins, expands and sets standards on the related legal principles and also references ethically related issues.

3.5.2 North Staffordshire Combined Healthcare NHS Trust is committed to achieving the following DPA, COP and IG objectives:

- The Trust regards all identifiable personal information relating to patients and staff as confidential and ensures any processing meets legal compliance;
- The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise;
- The Trust will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and common law confidentiality;

- The Trust will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Access to Health Records, Health and Social Care Act, Crime and Disorder Act, Protection of Children Act);

- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements.

3.6 Information Security

3.6.1 The aim of Information Security is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Trust.

3.6.2 North Staffordshire Combined Healthcare is committed to achieving the following Information Security and IG objectives:

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

- The Trust will establish and maintain an information asset register;

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

- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training;

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

3.7 Information Quality Assurance/Data Quality

3.7.1 The purpose of Data Quality is to ensure that the Trust has an approach which aims at ensuring consistently accurate information. It is also to ensure that the Trust is implementing an Information Quality Assurance Standards programme by raising awareness and meeting the Data Quality standards set by the former National Programme for IT.

3.7.2 North Staffordshire Combined Healthcare is committed to achieving the following Data Quality and IG objectives:

- 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;

- Where 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.

4 INFORMATION GOVERNANCE RESPONSIBILITIES AND ACCOUNTABILITY

4.1 The objective and focus of IG is that, via corporate partnership working, there is systematic management of the range of interrelated risks initiatives and work streams with the aim of addressing limitations thus raising standards that underpin the provision of high quality healthcare. The robust management of IG should lead to improvements in:

- Information handling/disclosure (both patient and corporate)

- Patient/public confidence in NHS

- Staff awareness, training and development

4.1.2 Strategically, IG requires a risk and control framework that functions with the Trust's existing Assurance Framework. The internal control mechanism is pivotal to managing risk and providing reasonable assurance to all stakeholders that there is a systematic process of identifying, evaluating and prioritising risk and managing them efficiently, effectively and economically. Operationally, the IG requirement for integration identifies and requires the active creation, involvement, or development of a number of staff roles and functions including:

4.2 Caldicott Guardian

4.2.1 The work of the Caldicott Guardian remains extremely important as the 'conscience' of the organisation. This role, an amalgamation of management and clinical responsibilities, helps to ensure the involvement of healthcare professionals in relation to achieving IG compliance.

4.2.2 As electronic records are rolled out across the NHS the Caldicott role will evolve further to encompass key new confidentiality management processes. Within the Trust, the Caldicott Guardian role is currently extremely broad. This role provides a pragmatic approach to addressing the Information Governance agenda locally.

4.2.3 Implementation of the NHS Confidentiality Code of Practice is the natural evolution of the Caldicott role and therefore the Caldicott Guardian has a key role in ensuring this is taken forward in the Trust by acting as an advocate for the principles of IG. Practically the Caldicott Guardian is required to:

- Oversee implementation of, and adherence to, the Caldicott principles

- Have responsibility for authorising access to patient information (this responsibility may also be delegated);

- Have responsibility for agreeing and authorising disclosure of patient information to other organisations via Information Sharing Protocols;

- Have responsibility for authorising the use of patient information for Clinical Research.

4.3 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) will be an Executive Director of the Trust who will be required to:-

- Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing IG Framework;

- Take ownership of risk assessment process for information risk, including review of the annual DSP Toolkit submission, in order to support and inform the Trust's Annual Governance Statement;

- To review and agree actions in respect of identified information risks;

- To ensure that the Trust's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff;

- To provide a focal point for the resolution and/or discussion of information risk issues;

- To ensure the Board is adequately briefed on information risk issues.

4.4 Data Protection Officer & IG Lead

4.4.1 Provides the organisation independent risk-based advice to support its decision-making in the appropriateness of processing Personal and Special Categories of Data within the principles of Data Protection Legislation Will be responsible for monitoring compliance with relevant laws and internal data protection policies.

4.4.2 Has particular responsibility for providing guidance on all areas of Information Governance, ensuring relevant legislation and guidance are incorporated into Trust practice via the IG Steering Group and providing leadership of the IG Team.

4.4.3 Support the Executive Director responsible for IG in the provision of leadership, strategic direction, and support for IG and to contribute to the achievement of Trust, Caldicott Guardian and IG objectives and business plans.

4.5 IG Manager

4.5.1 The key purpose of this role is to ensure the Trust successfully reports on and manages the risks associated with IG. To ensure the establishment of partnerships, corporate standards and a consistent and overarching Trust-wide view of, and ensure integration of and compliance with the DSP Toolkit.

4.5.2 Develop and implement strategies to achieve Information Governance and data quality standards, ensuring that those with responsibility for the achievement of standards under their responsibilities and implement changes as required.

4.6 Information Governance Steering Group

4.6.1 The Information Governance Steering Group, supported by the IG Lead and IG Manager, is required to ensure that the Trust has effective policies and management arrangements to identify risk and associated aspects of IG in accordance with the Trust's underpinning Information Governance Policy. (Ref: IG Steering Group Terms of Reference.)

- Steering Group members are chosen or nominated to provide expert IG knowledge or guidance, to ensure that all IG requirements are appropriately managed and to lead on specific work streams as identified by the steering group.

- To ensure that the Trust adheres to the fundamental aims of IG and the requirements.

- The Steering Group will identify the need for working groups as and when required.

- To ensure that the Trust undertakes or commissions annual assessments and audits of its Information Governance policies and arrangements.

- To establish an annual IG Improvement Plan, secure the necessary resources and monitor the implementation of that plan.

- To receive guidance from and support the Caldicott Guardian.

- Report any risk via the Trust Risk Register.

- To report Information Governance issues to the Quality Committee.

- To liaise with other Trust committees, working groups and programme boards in order to promote Information Governance issues.

- To receive and consider reports into breaches of confidentiality and security and where appropriate undertake or recommend remedial action.

4.7 Quality Committee

4.7.1 Part of the remit of the Quality Committee is to ensure that it is able to monitor and develop operational and strategic issues and influence decision making and the adoption of new procedures and policies. The group has a corporate responsibility to appreciate and support the requirements of IG are achieved by maintaining an understanding of IG related activities and ensuring that all opportunities are taken to establish IG responsibilities and accountabilities and improve standards and compliance.

- To assist in establishing a Trust wide culture of recognition of the importance of IG. To seek opportunities to facilitate the development of an organisational wide IG

responsibility ensuring managers actively seek opportunities for improved compliance.

- Assist in developing consistent corporate processes and policies for ensuring IG standards and compliance is formally addressed within all corporate projects and portfolios.

- To seek all opportunities to ensure that the Trust has effective policies and management arrangements covering all aspects of IG in line with this policy.

- Supported by the IG Lead, to monitor, develop and review corporate policies and systems to ensure that appropriate compliance is achieved with relevant legislation and guidance and that associated risk is successfully managed.

4.8 Clinical Governance Interface

4.8.1 Clinical Governance (CG) is the framework through which NHS organisations are accountable for continuously improving the quality of their services and safeguarding high standards of care. It is also the mechanism by which the Trust aims to ensure an individual and collective responsibility for developing and maintaining standards and creating an environment in which excellence in clinical care will flourish.

4.8.2 It is evident that CG and IG have areas of commonality both in approach and performance content and it is for this reason that specific IG standards will be included with the bi-annual Divisional CG assessment process. The IG element of the assessment will focus on:

- Issues (Education, Training, Development & Awareness);
- Use of Patient Identifiable Information;
- Management;
- Communications with Patients;

4.9 Divisional Management Teams, Senior Managers, Line Managers, Senior Medical and Nursing Staff

4.9.1 Strategically, senior staff have a corporate responsibility to appreciate and support the requirements of IG, achieved by maintaining an understanding of IG related activities and ensuring that all opportunities are taken to establish IG responsibilities and accountabilities and improve standards and compliance.

- The revision or creation of any policy or procedure referencing person identifiable information must appropriately reference both legal and NHS standards (e.g. Data Protection Legislation, NHS Confidentiality Code of Practice). Therefore, to facilitate referencing and to provide evidence of IG compliance all relevant policies must be issued for comments to the IG Steering Group before submission to Quality Committee etc. for approval.

- Senior Staff have a responsibility to ensure that the IG principles and supporting policy is known in their area, to assist staff with implementation, and to assist in IG compliance.

- Identify training needs and support staff to acquire appropriate knowledge and training.

4.10 All Staff

4.10.1 All staff, via their job roles, have responsibilities related to the IG components and therefore must be aware of the related underpinning work streams and standards that impact within their area of responsibility. Individual staff must ensure that any personal and corporate information is managed legally, securely and efficiently in order to assist in the delivery of the best possible care.

4.10.2 Any information governance incident where Trust policy and procedure has been violated by staff may be subject to formal disciplinary action under the Trust's Human Resource policy framework and, if considered sufficiently serious, may constitute grounds for dismissal.

5 EDUCATION, TRAINING AND AWARENESS

5.1 All staff must complete the mandated on line IG training (E-Learning for Health DSP Training) as part of the Trust's Statutory and Mandatory Training programme.

5.2 The Trust's Policies will be cascaded through the organisation's policy distribution system. Regular updates will also be provided through the Trust's internal communications systems.

6 MONITORING AND REVIEW

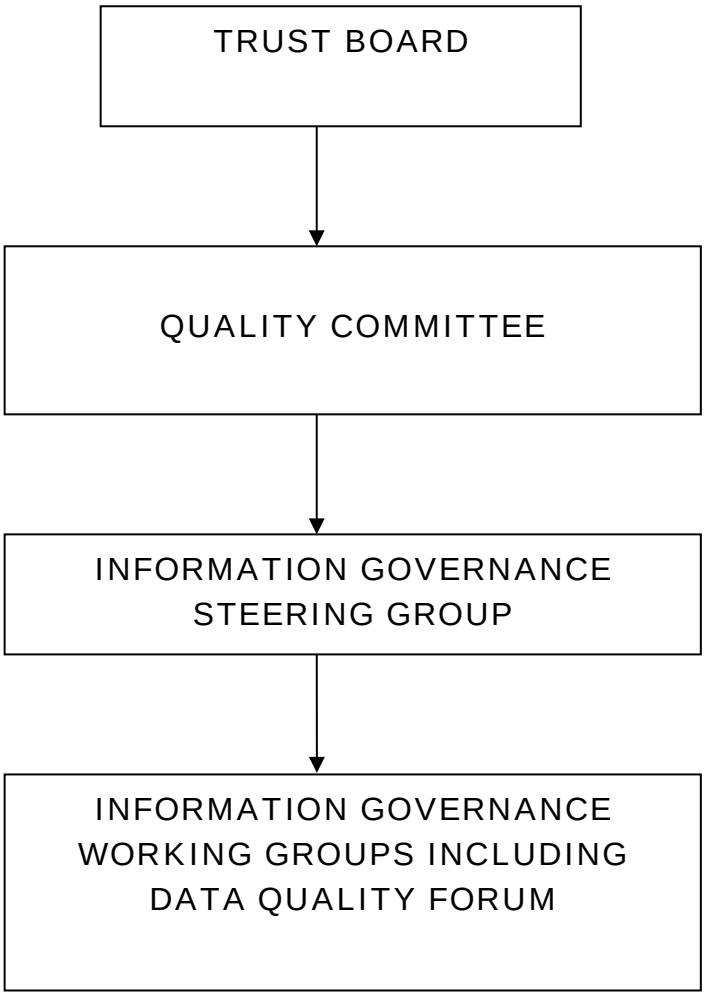
6.1 Compliance with this policy will be monitored through regular analysis of the Trust incident reports which are monitored by the Information Governance Steering Group.

6.2 In all instances, the application of the above policy will reference the particular needs and circumstances of each component or strand of work.

6.3 This policy will be reviewed annually by the Information Governance Steering Group as part of the review of IG arrangements carried out to meet the Information Governance Toolkit.

6.4 It is recognised that as related legislation or NHS standards are introduced the policy may need to be updated to reflect these minimum requirements.

Appendix 1
Accountability of Information Governance



Appendix 2
An overview of policies which link with Information Governance

Policy Number	Policy Title
4.18	Risk Management Policy
7.01	Confidentiality of Patient and Employee Personal Information
7.02	Subject Access Request Policy
7.03	Information Security & Data Protection Policy
7.05	One Staffordshire Information Sharing Protocol
7.07	Records Management Policy
7.10	Clinical Coding Policy
7.13	Data Quality Policy
7.14	Safe Haven Policy
7.16	IT Asset Management Policy
7.17	Policy on Health Records Standards and Clinical Data Management
7.18	Producing written clinical information for service users & carers
7.20	Information Lifecycle Management Strategy
7.21	Information Risk Security Policy