Information Governance & Data Security and Protection Policies

December 2019

These Policies have been developed by NHS Midlands & Lancashire Commissioning Support Unit (CSU), who act as NHS St Helens CCG's Information Governance Support Provider.

These Policies have been approved and adopted by NHS St Helens CCG and is applicable to all staff, including contractors and volunteers.

Consultation and Ratification Schedule	
Document Name:	Information Governance & Data Security and Protection Policies
Policy Number/Version:	3.0
Name of originator/author:	Midlands & Lancashire CSU Information Governance Team
Ratified by:	ELT Governance Committee
Name of responsible committee:	ELT Governance Committee
Date issued:	25.07.18 – **Appendix added 12/12/2019**
Review date:	June 2021
Date of first issue:	19th October 2016
Target audience:	All staff, including temporary staff and contractors, working for or on behalf of NHS St Helens CCG.
Purpose:	To set out the policy for Information Governance. To detail all staff responsibilities for Information Governance and the possible consequences of not following the guidance.
Action required:	All staff are required to read and sign the declaration at the back of the Staff Code of Conduct. Signing the declaration does not confirm that you are aware of everything but confirms that you have read it and know where to refer back to in the future if required.
Cross Reference:	Information Governance Handbook/Information Governance Staff Code of Conduct
Contact Details (for further information)	Midlands and Lancashire CSU Information Governance Team mlcsu.ig@nhs.net / 01782 872648

DOCUMENT STATUS

This is a controlled document. Whilst this document may be printed, the electronic version posted on the NHS St Helens CCG internet site is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the internet.

Version Control

Policy Name: Information Governance & Data Security and Protection Policies			
Version	Valid From	Valid To	Comment
1.0	19th October 2016	September 2018	New Policy superseding St Helens policy V3. Extended September 2017
1.1	5th June 2018	25th July 2018	Total redraft
2.0	25th July 2018	June 2021	Approved redraft
3.0	12th Dec 2019	June 2021	Addition of Appendix A (on advice of IG Team)

Glossary of Terms

Term	Acronym	Definition
Anonymisation		It is the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.
Business Continuity Plans	BCP	Documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical activities at an acceptable defined level.
Caldicott Guardian	CG	A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing.
CareCERT		NHS Digital has developed a Care Computer Emergency Response Team (**CareCERT**). CareCERT will offer advice and guidance to support health and social care organisations to respond effectively and safely to cyber security threats.
Clinical Commissioning Group	CCG	They are responsible for commissioning healthcare services in both community and hospital settings.
Commissioning Support Unit	CSU	A Commissioning Support Unit (CSU) is an Organisation. Commissioning Support Units provide Clinical Commissioning Groups with external support, specialist skills and knowledge to support them in their role as commissioners, for example by providing: Business intelligence services.
Code of Conduct		A set of rules to guide behaviour and decisions in a specified situation.
Continuing Healthcare	CHC	CHC is health care provided over an extended period of time for people with long-term needs or disability / people's care needs after hospital treatment has finished.
Common Law		The law derived from decisions of the courts, rather than Acts of Parliament or other legislation.
Care Quality Commission	CQC	This is an organisation funded by the Government to check all hospitals in England to make sure they are meeting government standards and to share their findings with the public.

Term	Acronym	Definition
Data Controller		The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor		A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Act 1998	DPA 1998	An Act for the regulation of the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information.
Data Protection Act 2018	DPA18	Act replaced DPA 1998 above.
Data Protection Impact Assessment	DPIA	A method of identifying and addressing privacy risks in compliance with GDPR requirements.
Data Protection Officer	DPO	A role with responsibility for enabling compliance with data protection legislation and playing a key role in fostering a data protection culture and helps implement essential elements of data protection legislation.
Data Security and Protection Toolkit	DSP Toolkit	From April 2018, the DSP Toolkit will replace the Information Governance (IG) Toolkit as the standard for cyber and data security for healthcare organisations.
Data Sharing Agreement		A contract outlining the information that parties agree to share and the terms under which the sharing will take place.
Freedom of Information Act 2000	FOI	The Freedom of Information Act 2000 provides public access to information held by public authorities.
General Data Protection Regulation	GDPR	The General Data Protection Regulation (GDPR), agreed upon by the European Parliament and Council in April 2016, will replace the Data Protection Directive 95/46/ec in Spring 2018 as the primary law regulating how companies protect EU citizens' personal data.
Information Asset Owner	IAO	Information Asset Owners are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'.
Information Assets		Includes operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications

Information Commissioner's Office	ICO	The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Individual Funding Requests	IFR	Application to fund treatment or service not routinely offered by NHS.
Key Performance Indicators	KPI's	Targets which performance can be tracked against.
Pseudonymisation		The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Record Lifecycle		Records life-cycle in records management refers to the stages of a records "life span": from its creation to its preservation (in an archives) or disposal.
Senior Information Risk Owner	SIRO	Board member with overall responsibility for: • The Information Governance policy • Providing independent senior board-level accountability and assurance that information risks are addressed • Ensuring that information risks are treated as a priority for business outcomes • Playing a vital role in getting the institution to recognise the value of its information, enabling its optimal effective use.
Subject Access Request	SAR	A subject access request (SAR) is simply a written request made by or on behalf of an individual for the information which he or she is entitled to ask for under the Data Protection Act.

Table of Contents

Information Governance Policy

Purpose of Policy

This overarching Data Security and Protection or Information Governance policy provides an overview of the organisation's approach to information governance and includes data protection and other related information governance policies; and details about the roles and management responsible for data security and protection in the organisation.

Introduction

Information is the most important asset available to an organisation and therefore all organisations must have robust arrangements for Information Governance (IG) which are reviewed annually and described in the new Data Security and Protection Toolkit (DS&PT).

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

The policies will provide assurance to the CCG and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

Through the action of approving the policy and its associated supporting documents, the Board provides an organisational commitment to its staff and the public that information will be handled within the identified framework.

The role of the CCG is to commission healthcare, both directly and indirectly, so that valuable public resources secure the best possible outcomes for patients. In doing so, the CCG will seek to meet the objectives prescribed in the NHS Act 2006 and the Health & Social Care Act 2012 and to uphold the NHS Constitution. The objective of this policy is to ensure that people who work for the CCG understand how to look after the information they need to do their jobs, and to protect this information on behalf of patients.

General Data Protection Regulations/Data Protection Act 2018

The EU General Data Protection Regulation (GDPR) was approved in 2016 and became directly applicable as law in the UK from 25th May 2018 as did the Data Protection Act 2018 (DPA18) and fills in the gaps of the GDPR, addressing areas in which flexibility and derogations are permitted.

The new GDPR/DPA18 is underpinned by a number of data protection principles which drive compliance. While the data protection principles under the GDPR/DPA18 are similar to those found in in the DPA 1998, certain concepts are more fully developed.

Six Principles of the General Data Protection Regulations/Data Protection Act 2018 (GDPR/DPA18)

- First. Lawful, fair and transparent processing – this principle emphasizes transparency for all EU data subjects. When the data is collected, it must be clear as to why that data is being collected and how the data will be used. Organisations must also be willing to provide details surrounding the data processing when requested by the data subject. For example, if a data subject asks who the data protection officer is at that organisation or what data the organisation has about them, that information needs to be available.

- Second. Purpose limitation – this principle means that organisations need to have a lawful and legitimate purpose for processing the information in the first place. Consider organisations that require forms with 20 data fields, when all they really need is a name, email, address and maybe a phone number. Simply

put, this principle says that organisations shouldn't collect any piece of data that doesn't have a specific purpose, and those who do can be out of compliance.

- Third. Data minimisation – this principle instructs organisations to ensure the data they capture is adequate, relevant and not excessive. In this day and age, businesses collect and compile every piece of data possible for various reasons, such as understanding customer buying behaviors and patterns or remarketing based on intelligent analytics. Based on this principle, organisations must be sure that they are only storing the minimum amount of data required for their purpose

- Fourth. Accurate and up-to-date – this principle requires data controllers to make sure information remains accurate, valid and fit for purpose. To comply with this principle, the organisation must have a process and policies in place to address how they will maintain the data they are processing and storing. It may seem like a lot of work, but a conscious effort to maintain accurate customer and employee databases will help prove compliance and hopefully also prove useful to the business.

- Fifth. Kept for no longer than necessary – this principle discourages unnecessary data redundancy and replication. It limits how the data is stored and moved, how long the data is stored, and requires the understanding of how the data subject would be identified if the data records were to be breached. To ensure compliance, organisations must have control over the storage and movement of data. This includes implementing and enforcing data retention policies and not allowing data to be stored in multiple places. For example, organisations should prevent users from saving a copy of a customer list on a local laptop or moving the data to an external device such as a USB. Having multiple, illegitimate copies of the same data in multiple locations will cause major compliance problems.

- Sixth. Appropriate security measures – this principle protects the integrity and privacy of data by making sure it is secure (which extends to IT systems, paper records and physical security). An organisation that is collecting, and processing data is now solely responsible for implementing appropriate security measures that are proportionate to the risks and rights of individual data subjects. Negligence is no longer an excuse under GDPR/DPA18, so organisations must spend an adequate amount of resources to protect the data from those who are negligent or malicious. To achieve compliance, organisations should evaluate how well they are enforcing security policies, utilizing dynamic access controls, verifying the identity of those accessing the data and protecting against malware/ransomware.

For information the GDPR also introduced the principle of accountability:

- Accountability and liability – this principle ensures that organisations can demonstrate compliance. Organisations must be able to demonstrate to the governing bodies that they have taken the necessary steps comparable to the risk their data subjects face. To ensure compliance, organisations must be sure that every step within the GDPR strategy is auditable and can be compiled as evidence quickly and efficiently. For example, GDPR requires organisations to respond to requests from data subjects regarding what data is available about them. The organisation must be able to promptly remove that data, if desired. Organisations not only need to have a process in place to manage the request, but also need to have a full audit trail to prove that they took the proper actions.

Caldicott Principles

The Caldicott Committee Report on the Review of Patient-Identifiable Information 1997 found that compliance with confidentiality and security arrangements was patchy across the NHS and identified six good practice principles for the health service when handling patient information. A further Caldicott review was published in March 2013 which amended the Caldicott Principles, as follows

- Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

- Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

- Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

- Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

- Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

- Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

- The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Appointment of Data Protection Officer

Under GDPR/DPA18, Data Protection Officers (DPO's) will be at the heart of this new legal framework for all Health and Social care organisations facilitating compliance with the provisions of the GDPR.

It is **mandatory** for data controllers and processors to designate a DPO. It is especially important for organisations to nominate a DPO where it is processing personal and sensitive information on a large scale.

It would also be important to ensure that the DPO contact details are available in accordance with the requirements such as in fair processing notices.

For public authorities, DPO's are also required to have knowledge of administrative rules and procedures of the organisation.

The GDPR/DPA18 requires that organisations involve the DPO, "in all issues which relate to the protection of personal data". It is therefore crucial that the DPO is involved from the earliest stage possible in all issues relating to data

protection.

In relation to Data Protection Impact Assessments (DPIA), the GDPR/DPA18 explicitly provides for the early involvement of the DPO and specifies that the controller shall seek the advice of the DPO when carrying out such impact assessments.

Ensuring that the DPO is informed and consulted at the outset will facilitate compliance with the DPA18, promote a privacy by design approach and should therefore be standard procedure within an organisations governance and procurement procedures.

In addition, it is important that the DPO be seen as a discussion partner within the organisation and that they are part of the relevant working groups dealing with data processing activities within the organisation.

Due to the large volume of high risk sensitive data being processed within the NHS the concept of the Data Protection Officer role is well embedded due to the mandated requirement to comply with the existing Data Protection Act through the Information Governance Toolkit. This means that the roles, tasks and responsibilities are already undertaken within the CCG due to the maturity of Information Governance compliance in the CCG and the wider National Health Service.

Within NHS St Helens CCG the DPO role has been delegated to the Associate Director of Corporate Governance which includes compliance responsibility for GDPR/DPA18, FOIA and data security.

Organisations should continue to ensure that the Head of Information Governance or the designated representative:

- Is invited to participate regularly in meetings of senior and middle management where data processing activities are discussed, for example the Finance, Governance & Risk Committee.
- Are consulted where decisions with data protection implications are taken. All relevant information must be passed on to the IG team in a timely manner to allow them to provide adequate advice.
- The opinion of the IG team should always be given due weight. In case of disagreement, the GDPR/DPA18 recommends, as good practice, to document the reasons for not following the DPO or IG team's advice.
- The DPO/IG team must be promptly consulted once a data breach or another incident has occurred, for example when incidents occur.

Resources

The GDPR/DPA18 requires that the organisation support the DPO function by providing resources necessary to carry out tasks and access to personal data and processing operations to maintain their expert knowledge, this could be through:

- Active support for the DPO function by senior management at Board Level
- Sufficient time to fulfil their duties
- Adequate support in terms of financial resources, infrastructure and premises
- Official communication of the role and support
- Continuous training to stay up to date within the field of Data Protection

It may also be necessary to set up a DPO team.

Scope

This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. The policy also applies to all third parties and others authorised to undertake work on behalf of the CCG

Responsibilities:

Organisation (Accountable Officer)

Overall accountability for procedural documents across the organisation lies with the CCG Strategic Director; People's Services/Clinical Accountable Officer. As the Accountable Officer has overall responsibility for establishing and maintaining an effective document management system and the governance of information, meeting statutory requirements and adhering to guidance issued in respect of information governance and procedural documents.

SIRO

NHS St Helens CCG has appointed the Chief Finance Officer as Senior Information Risk Owner (SIRO), who will:

- Take overall ownership of the organisation's Information Risk Policy
- Act as champion for information risk on the Board and provide written advice to the Accountable Officer on the content of the organisation's annual governance statement in regard to information risk
- Understand how the strategic business goals of the CCG and how other NHS organisations' business goals may be impacted by information risks, and how those risks may be managed
- Implement and lead the NHS Information Governance Risk Assessment and Management processes within the CCG
- Advise the Board on the effectiveness of information risk management across the CCG and
- Receive training as necessary to ensure they remain effective in their role as SIRO

Caldicott Guardian

NHS St Helens CCG has appointed the CCG Strategic Director; People's Services/Clinical Accountable Officer as Caldicott Guardian, who will:

- Ensure that the CCG satisfies the highest practical standards for handling patient identifiable information
- Facilitate and enable appropriate information sharing and make decisions on behalf of the CCG following advice on options for lawful and ethical processing of information, in particular in relation to disclosures
- Represent and champion Information Governance requirements and issues at Board level
- Ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff, and
- Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS

Data Protection Officer

NHS St Helens CCG has also appointed the Associate Director of Corporate Governance as the Data Protection Officer (see section above about this new role).

Information Asset Owners

Information Asset Owners are accountable for the application of this policy to the information assets that they 'own':

- Lead and foster a culture that values, protects and uses information for the benefit of patients
- Know what information comprises or is associated with the asset and understands the nature and justification of information flows to and from the asset
- Know who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with policy
- Understand and address risks to the asset and providing assurance to the SIRO
- Ensure there is a legal basis for processing and for any disclosures, and
- Refer queries about any of the above to the Associate Directorate: Corporate Governance

Line Managers

Line managers will take responsibility for ensuring that these policies are implemented within their department or area of responsibility.

User

It is the responsibility of each employee to adhere to the policies.

All staff must make sure that they use the organisation's IT systems appropriately and in accordance with the IG Handbook/Code of Conduct.

Finance, Governance & Risk Committee

NHS St Helens CCG has established a Finance, Governance & Risk Committee (FGR) to monitor and co-ordinate implementation of the policies, the new Data Security and Protection Toolkit requirements and other information related legal obligations.

Information Governance Team

The MLCSU Information Governance Team will provide expert advice and guidance to all staff on all elements of Information Governance. The team is responsible for:

- Providing advice and guidance on Information Governance issues to all staff
- Developing information governance policies and procedures
- Developing information governance awareness and training programmes for staff
- Ensuring compliance with GDPR/DPA18, Information Security and other information related legislation
- Providing support to the team who handle freedom of information and subject access requests
- Providing support to Caldicott Guardian and Senior Information Risk Owner for information governance issues

Information Governance Training

All staff are mandated to undertake the Data Security Awareness Level 1 e-learning module within their 1st year of employment. For subsequent information governance training, staff will undertake the MLCSU IG refresher module either as face to face training or via the Learning Management System (LMS).

Data Security and Protection Toolkit

From April 2018 the Data Security and Protection Toolkit (DSP Toolkit) replaces the Information Governance Toolkit (IG Toolkit). It will form part of a new framework for assuring that organisations are implementing the ten data security standards and meeting their statutory obligations on data protection and data security recommended in the government's response to the National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs and the Care Quality Commission's Review 'Safe Data, Safe Care'.

The ten data security standards apply to all health and care organisations. When considering data security as part of the well-led element of their inspections, the Care Quality Commission (CQC) will look at how organisations are assuring themselves that the steps set out in this document are being taken.

CCGs, as discrete NHS organisations responsible for their corporate IT services, must comply with the requirements.

Data Security and Protection Requirements – NHS Organisations

Leadership Obligation 1	
People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles	
Data Security Standard 1	All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful and appropriate purposes
Data Security Standard 2	All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
Data Security Standard 3	All staff complete appropriate annual data security training and pass a mandatory test, provided through the redesigned Data Security and Protection Toolkit (or provide similar via in-house training programmes)

Leadership Obligation 2	
Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses	
Data Security Standard 4	Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
Data Security Standard 5	Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security
Data Security Standard 6	Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
Data Security Standard 7	A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management

Leadership Obligation 3	
Technology: Ensure technology is secure and up-to-date.	
Data Security Standard 8	No unsupported operating systems, software or internet browsers are used within the IT estate.
Data Security Standard 9	A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually
Data Security Standard 10	IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards

Supporting policies and procedures to meet their information governance, data security and protection obligations and enable the CCG to fulfil its information governance responsibilities. These policies provide a framework to bring together all of the requirements, standards and best practice that apply to the handling of confidential, business sensitive and personal information and include:

- Data Protection
- Data Quality
- Records Management
- Access to Information
- Freedom of Information
- IT/Network Security (Links to IT provider Policies)

Policy Review

These policies will be reviewed every 3 years or earlier if required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance.

Data Protection Policy

Introduction

NHS St Helens CCG needs to collect personal confidential information about people with whom it deals in order to carry out its business and provide its services for healthcare. Such people include patients, employees (present, past and prospective), suppliers and other business contacts. The information includes name, address, email address, date of birth, private and confidential information, and sensitive information.

In addition, the CCG may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or other digital media, on hardcopy, paper or images, including CCTV) this personal information must be dealt with properly to ensure compliance with GDPR/DPA18.

The lawful and proper treatment of personal information by the CCG is extremely important to the success of our business and in order to maintain the confidence of our service users and employees. We ensure that personal information is held lawfully and correctly and in line with this policy.

Keeping data subjects informed

We are required to let patients and other data subjects know what Information we collect about them, how we will use it and who we may share it with.

There are a number of methods for achieving this, for example information is posted on our public facing website through our privacy notice.

Data quality and reuse

We will seek to maintain standards of information quality and avoid duplication, inaccuracy and inconsistencies across personal information. We will maintain a comprehensive records management policy as part of this overarching policy, see below, in order to help avoid excessive retention or premature destruction of personal information.

We will only use personal information where strictly necessary. Wherever it is possible to use anonymised data this will be preferred.

Data subjects' rights

We have a records management policy which ensures that individuals can exercise rights over their own personal data in line with GDPR/DPA18. Access to the records of the deceased is also covered under the remit of this policy, though these fall outside of the GDPR/DPA18 and are dealt with in line with the Access to Health Records Act 1990 and the Freedom of Information Act 2000.

Record of Processing Activities

As part of its compliance with GDPR/DPA18 and to provide assurance to its regulatory bodies we must maintain an internal record of processing activities which includes the following:

- Purposes of the processing
- Description of the data processed
- Details of who we send personal data to
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place
- Description of technical and organisational security measures

Security

Personal data should be kept secure at all times. We will ensure that there are adequate policies and procedures, including the new IG handbook and Code of Conduct, in place to protect against unauthorised access and against loss, destruction and damage.

Data Quality Policy

Introduction

NHS St Helens CCG is committed to ensuring the quality of its data, to promote effective decision making and patient safety.

High quality information means better patient care and patient safety, and there could be potentially serious consequences if information is not correct and up to date, both for patients and for the CCG as a whole.

Management information produced from patient data is essential for the efficient running of the CCG and to maximise utilisation of resources for the benefit of patients and staff. It supports making effective decisions about the deployment of resources, and in demonstrating the value of the services provided by the CCG.

The CCG requires accurate, timely and relevant patient information to support:

- The delivery of effective, safe patient care
- The delivery of its core business objectives
- The monitoring of activity and performance for internal and external management purposes
- Clinical governance and clinical audit
- Service agreements and contracts
- Healthcare planning
- Accountability
- Compliance with Data Protection Act 2018
- To be able to evidence compliance with regulatory requirements
- Support effective decision making with regards to the deployment of resources

The key obligations upon staff to maintain accurate records relate to:

- Department of Health, Information Governance requirements
- Legal - GDPR/DPA18
- Care Records Guarantee
- Freedom of Information Act (2000)
- Environmental Information Regulations (2000)
- Access to Health Records Act (1990)
- Contractual (contracts of employment)
- Ethical (Professional codes of practice)
- Policy (Records Management Policy, Information Governance Policy)
- NHS Constitution

NHS St Helens CCG is committed to ensuring and improving where possible the quality of data it uses for all purposes.

Purpose

The purpose of this policy is to set out what is required by all staff in order to ensure the quality of data used across the CCG.

Responsibility for data quality rests with the Chief Finance Officer.

It is the responsibility of all staff to ensure the information they generate is legible, complete, accurate, relevant, accessible and recorded in a timely manner. The quality of information produced can have a significant impact on the quality of services that we provide.

Data Quality is essential for:

- Efficient delivery of patient care e.g. by ensuring that patients are given appointments and admission dates based on clinical priority and length of waiting time.
- Clinical governance and minimising clinical risk e.g. wrong patient, wrong treatment.
- Management information to enable decisions to be made on the basis of sound information, operational and strategic, local and national.
- Performance measurement against national trends and trends over time, so that we can continually plan improvements for our patients.
- As a foundation on which future investment and strategic decisions will be based.
- To support clinical audit and research and development, with a view to improving patient care in the future.

All staff need to be able to rely on the accuracy of the information available to them, in order to provide timely and effective services regardless of whether they are patient facing or central support functions.

To achieve this, all staff need to understand their responsibilities with regard to accurate recording of patient data, whether on a computer system or on paper, e.g. case notes.

Data Quality Standards

The CCG data quality standards are:

Accurate and up to date:

All data must be correct and accurately reflect what happened. Therefore, all reference tables including GPs and postcodes must be updated regularly usually within a month of publication. Every opportunity must be taken to check a patient's demographic details with the patient themselves at every in-patient, out-patient and any associated service in accordance with service area specific Standard Operating Procedures (SOPs) as inaccurate demographics may result in important letters being mislaid, or the incorrect identification of patients. However, it is important to note that the accuracy and timeliness of data does not just relate to patients.

Valid:

Data should be within an agreed format which conforms to recognised national or local standards. Codes must map to national values and wherever possible, computer systems should be programmed to only accept valid entries.

Complete:

Data should be captured in full. All mandatory data items within a data set should be completed and default codes will only be used where appropriate, not as a substitute for real data. The use of mandatory data items on the computer systems is to be encouraged but only where this would not cause undue delay. For key data items which are not mandatory on the computer system, it is vital that a list of records with missing items can be produced, to be actioned later.

Timely:

Data should be collected at the earliest opportunity; recording of timely data is beneficial to the treatment of the patient. All data will be recorded to a deadline which will ensure that it meets national reporting and extract deadlines

Defined and consistent:

The data being collected should be understood by the staff collecting it and data items should be internally consistent. Data definitions should be reflected in procedure documents.

Coverage:

Data will reflect the work of the CCG and not go unrecorded. Spot checks and comparison of data between months can highlight potential areas of data loss. Staff should be cognisant that if something is not recorded there is no auditable proof that something occurred, and as such could be challenged.

Free from duplication and fragmentation:

Patients should not have duplicated or confused patient records, and where possible data should be recorded once and staff should know exactly where to access the data. Where a duplicate record is created, for example in the event that a record is misplaced, records should be merged once the original is found.

Security and confidentiality:

Data must be stored securely and processed in line with relevant legislation and local policy in relation to confidentiality. All staff must pay due regard to where they record information, what they record, how they store it and how they share information ensuring they comply with national and local requirements, policies and procedures.

How Data Quality can be improved

NHS St Helens CCG acknowledges that good quality data can be achieved by careful monitoring and error correction, but it is more effective and efficient for data to be entered correctly first time. In order to achieve this, good procedures must exist so that staff can be trained and supported in their work.

Information Asset Owners are responsible for ensuring that there are specific policies or procedures in place in relation to all information assets under their control, which set out as a minimum, when the information asset should be used, how it should be used and by whom and how the quality of data recorded will be monitored.

Where appropriate Information Asset Owners must ensure that training is available for staff to use the asset, and that information risks associated with each asset are actively identified, and being mitigated, ensuring that they provide assurance to the SIRO.

Procedures need to be reviewed at least every three years or in response to changes in legislation, best practice etc., to take account of any changes in national standards and definitions.

Tight version control is essential so that staff in all parts of the CCG are using the same procedures which reflect current data definitions.

Records Management Policy

Introduction

This policy sets out the principles of records management for the CCG and provides a framework for the consistent and effective management of records that is standards based and fully integrated with other information governance initiatives within the CCG.

Records management is necessary to support the business of the CCG and to meet its obligations in terms of legislation and national guidelines.

The policy is based on guidance from the NHS Digital/Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016 and the Records Management Roadmap issued by NHS Digital. Both documents provide guidelines for good practice in managing all types of NHS records and highlight the responsibilities of all staff for the records they create or use.

NHS St Helens CCG has a statutory obligation to maintain accurate records of their activities and to make arrangements for their safe keeping and secure disposal. All records created in the course of the business of the CCG are public records under the terms of the Public Records Act 1958.

Effective records management is an essential requirement of the commissioning obligations of the CCG. It also recognises the importance of good records management practices to ensure:

- The right information is available at the right time.
- Authentic and reliable evidence of business transactions.
- Support for decision making and planning processes.
- Better use of physical and server space.
- Better use of staff time.
- Compliance with legislation and standards.
- Reduced costs.

Purpose and Scope

This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. The policy also applies to all third parties and others authorised to undertake work on behalf of the CCG.

NHS St Helens CCG records are part of the organisation's corporate memory, providing the evidence of actions and decisions and representing a vital asset to support daily functions and operations and to:

- provide guidance to staff to carry out their corporate and personal record management responsibilities to support high quality patient care.
- support the organisation and staff in meeting their obligations in terms of legislation and national good practice guidance.
- provide effective governance arrangements for record management, also known as 'information lifecycle management'.

Definitions

Records: Recorded information in any form or medium, created or received and maintained by an organisation or person in the transaction of business or the conduct of affairs.

Health Records: records which consists of information relating to the physical or mental health of an individual and has been made by or on behalf of a health professional in connection with that care.

Corporate Records: records which relate to the corporate business of the CCG such as accounts, minutes and meeting papers and legal and other administrative documents. They may contain personal identifiable information, for example personnel files and should be treated with the same degree of care and security as patient/service user records.

Records Management: is a discipline which utilises administrative systems to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the CCG and preserving an appropriate historical record.

Records Lifecycle: a period a record exists from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as semi-active or closed records which may be referred to occasionally) and finally either confidential destruction or archival preservation.

Records Management

Records Creation

All records created in the CCG must be created in a manner that ensures that they are clearly identifiable, accessible, and can be retrieved when required.

All records created in the CCG must be; authentic, credible, authoritative and adequate for the purposes for which they are kept. They must correctly reflect what was communicated, decided or undertaken.

Adequate records must be created where there is a need to be accountable for decisions, actions, outcomes or processes. For example, the minutes of a meeting, a clinician's examination of a patient, the payment of an account or the appraisal of a member of staff.

Records Use and Maintenance

All staff have a duty for the maintenance and protection of records they use. Only authorised staff should have access to records.

The identification and safeguarding of vital records necessary for business continuity should be included in all business continuity /disaster recovery plans.

Any incidents relating to records, including the unavailability and loss, must be reported as an incident using the CCG incident reporting system.

Accuracy of statements i.e. record keeping standards, should pay particular attention to stating facts not opinions.

Records Tracking

Accurate recording and knowledge of the whereabouts of all records is essential if the information they contain is to be located quickly and efficiently. One of the main reasons records are misplaced or lost is that the next destination is not formally recorded. All services/departments should ensure they have appropriate tracking systems and audit trails in place to monitor the use and movement of records.

Records Transportation

When records are being transported, whether they are electronic or paper, care should be taken to ensure the safe transition to the new location, whether this be temporary or permanent.

Records Storage

Records storage areas must provide storage which is safe from unauthorised access but which allows maximum accessibility to the records commensurate to its frequency of use.

The following factors must be taken into account:

- Compliance with Health and Safety and fire prevention regulations.
- Degree of security required.
- User needs.
- Type of records stored.
- Size & quantity of records.
- Usage and frequency of retrievals.
- Ergonomics, space, efficiency and price.

Inactive records sent for storage off-site (such as Iron Mountain) must be boxed and include a retention date. The Information Asset Owner is responsible for keeping an accurate and up-to-date inventory of all records sent off-site.

Retention

The minimum length of time that a record is retained by the CCG depends on the type of record. The CCG has adopted the minimum retention schedules published in the Records Management Code of Practice for Health and Social Care 2016.

Records, in whatever format they are held, may be retained for longer than the minimum retention periods, but should not normally be kept for more than 30 years.

Requests for extended preservation are subject to approval by the Finance, Governance & Risk Committee. This may only happen on grounds of historical archival value, relevance to research or other preserved records.

Information Asset Owners are responsible for determining if a record for which they are accountable should be retained for longer than the minimum retention period. This should be listed in a local retention schedule and communicated to all Information Asset Administrators. Local retention schedules must be approved by the Finance, Governance & Risk Committee before implementation.

Disposal and destruction of records

For records that have reached their minimum retention period and there is no justification for continuing to hold them, they should be disposed of appropriately.

Paper records of a confidential nature should either be shredded using a cross shredder to DIN standard 4 or put in confidential waste that is appropriately destroyed by a company contracted to the organisation. Electronic records must be deleted from the device and not simply moved into the Trash folder, known as double deleting.

Access to Information Policy (Subject Access Requests - SAR)

Introduction

All living individuals have the right under the new Data Protection Regulations (GDPR/DPA18), subject to certain exemptions, to have access to their personal records that are held by the CCG. This is known as a 'subject access request' (SAR).

The GDPR/DPA18 applies only to living persons but there are limited rights of access to personal data of deceased persons under the Access to Health Records Act 1990

Requests may be received from members of staff, service users or any other individual who the CCG has had dealings with and holds data about that individual.

This will include information held both electronically and manually and will therefore include personal information recorded within electronic systems, spreadsheets, databases or word documents and may also be in the form of photographs, x-rays, audio recordings and CCTV images etc.

Anyone making such a requested is entitled to be given a description of the information held, what it is used for, who might use it, who it may be passed on to, where the information was gathered from.

Under GDPR individuals must also be provided with information on the expected retention periods of the information held, the right to request rectification or erasure of processing or raise an objection to the processing altogether.

GDPR/DPA18 changes to SAR

Under GDPR/DPA18 the right to make a SAR will be very similar, with the key changes including:

- Abolition of the £10 administration fee (although "reasonable" fees can be charged for an excessive request or for further copies).
- Information must be provided without delay and at the latest within one month of receipt.
- Higher fines for failing to comply. The maximum fine that can be issued by the Information Commissioner (ICO) is 4% of global turnover or 20 million euros, whichever is higher, and individuals also retain the right to pursue a claim in court.

Scope and Purpose

This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. The policy also applies to all third parties and others authorised to undertake work on behalf of the CCG.

The purpose of this policy is to provide a guide to all staff on how to deal with subject access requests received and advise service users and other individuals on how and where to make requests.

What is a SAR

Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them. However, subject access goes further than this and an individual is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;

- given a copy of the personal data; and
- given details of the source of the data (where this is available)

Personal data is information that relates to an individual who can be identified either directly or indirectly and includes any expression of opinion about the individual and any indication of the intentions of the information holder or any other person in respect of the individual.

Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR, other conditions to consider:

- All clinical data should be reviewed by a clinician and consideration should be given to redacting any information likely to cause serious harm to the mental or physical health of any individual
- Information supplied by third parties e.g. family members should usually be redacted
- Data and information held from other agencies may be disclosable but should be discussed with the originating body first
- Any information subject to Legal Professional Privilege should not be disclosed
- Information should not be disclosed where there is a statutory or court restriction on disclosure e.g. adoption records
- References written for current or former employees are exempt (but not those received from third parties)
- In the case of a deceased individual's records, information should not be disclosed where the entry in the records makes it clear that the deceased expected the information to remain confidential
- A personal record may also contain reference to third parties and redaction should be considered by balancing the GDPR/DPA18 rights of all parties

Recognising a SAR

A SAR must be made in writing; however, the requestor does not need to mention Data Protection/GDPR or state that they are making a SAR for their request to be valid. They may even refer to other legislation, for example, the Freedom of Information Act 1998, but their request should still be treated according to this policy.

The following are examples of formal subject access requests:

- Please send me a copy of my HR file, or medical records
- I am a solicitor acting on behalf of my client and request a copy of their medical record (an appropriate authority is enclosed)
- The police state that they are investigating a crime and provide an appropriate form requesting information signed by a senior police officer

Requests should be dealt with within a maximum of one month under GDPR subject to the necessity to seek clarification. It is possible to extend this timescale by a further two months where requests are complex however if this is the case the CCG must inform the individual within one month of the request and explain why the extension is necessary.

NHS best practice recommends disclosure within 21 days where a record has been added to in the last 40 days.

The Common Law Duty of Confidentiality extends beyond death. Certain individuals have rights of access to deceased records under the Access to Health Records Act 1990:

- The patient's personal representative (Executor or Administrator of the deceased's estate)
- Any person who may have a claim arising out of the patient's death

A Next of Kin has no automatic right of access, but professional codes of practice allow for a clinician to share information where concerns have been raised. Guidance should be sought from the Caldicott Guardian in relation to requests for deceased records.

A SAR can be made via any of, but not exclusively, the following methods:

- Email
- Fax
- Post
- Social media
- CCG website

Where an individual is unable to make a written request, it is the Department of Health view that in serving the interest of patients it can be made verbally, with the details recorded on the individual's file.

Requests made about or on behalf of other individuals

A third party, e.g. solicitor, may also make a valid SAR on behalf of an individual.

Where a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individuals consent or evidence of a legal right to act on behalf of that individual e.g. power of attorney must be provided by the third party.

Requests on behalf of a child

Even if a child is too young to understand the implications of subject access rights, information about them is still their personal information and does not belong to anyone else, such as a parent or guardian.

So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If the clinician responsible for the child's treatment plan is confident that the child can be considered competent under Gillick/Fraser guidelines, has the capacity to understand their rights and any implications of the disclosure of information, then the child's permission should be sought to action the request.

Further clarification guidance is still awaited in relation to the rights of children under GDPR/DPA18.

The Information Commissioner (ICO) has indicated that in most cases it would be reasonable to assume that any child that is aged 12 years or more would have the capacity to make a subject access request and should therefore be consulted in respect of requests made on their behalf.

The Caldicott Guardian should also be consulted on whether there is any additional duty of confidence owed to the child or young person as it does not follow that, just because a child has capacity to make a SAR, that they also have the capacity to consent to sharing their personal information with others as they may still not fully understand the implications of doing so.

Requests for personal information – police/HMRC

Requests for personal information may be made by the above authorities for the following purposes:

- The prevention or detection of crime;
- The capture or prosecution of offenders; and

- The assessment or collection of tax or duty.

A formal documented request signed by a senior officer from the relevant authority is required before proceeding with the request.

The request must make it clear that one of the above purposes is being investigated and that not receiving the information would prejudice the investigation.

These types of requests must be considered by a senior manager or the SAR team before any decision or action is taken to release information.

Court Orders

All Court Order requesting personal information about an individual must be complied with.

Subject Access Request Process

Requests for information held about an individual must be directed to the SAR team:

mlcsusars@nhs.net

Midlands and Lancashire CSU SAR Team, Liverpool Innovation Park Second Floor (Building 2), 360 Edge Lane,

Liverpool L7 9NJ

It is important that a SAR is identified and sent to the SAR team quickly in order for the request to be responded to within one month or receipt.

Responding to requests

A detailed Standard Operating Procedure SoP has been produced which gives full details as to how the CCG responds to individual SAR, access to the SoP is available through the SAR team.

It is essential though that a log of all requests received is maintained and includes:

- Date received
- Date response due (within one month)
- Applicants details
- Information requested
- Exemptions applied, if applicable
- Details of decisions to disclose information without the subject's consent (if applicable)
- Details of information to be disclosed and the format in which they were supplied
- When and how supplied (for example, hard copy and by post)

Performance monitoring

The CCG will ensure that monitoring and evaluation of the implementation of SAR takes place on a regular basis. The SAR team will report progress reports to the Finance, Governance & Risk Committee and will include following:

- Number of requests
- Incidents/Breaches in response times (detailed exception reports)
- Complaints

Freedom of Information (FOI) Policy

Introduction

The Freedom of Information Act (2000) came into effect for all public authorities in January 2005. Since then, all requests for information have had to be answered in accordance with the Freedom of Information (FOI) Act 2000 or the Environmental Information Regulations 2004 (EIR).

The Freedom of Information Act gives a general right of access to all types of recorded information held by public authorities. Disclosures are subject to the application of relevant exemptions contained within the Act.

Under the Act, NHS St Helens CCG must consider all requests for recorded information it receives and must:

- Inform the applicant whether the information is held and
- Supply the requested information subject to the application of relevant exemptions contained within the Act

We remain committed to promoting a culture of openness and accountability to enable you to have a greater understanding of how we carry out our duties, how we make decisions and how we spend public money.

The FOIA is fully retrospective and covers all information held in a recorded format. The deadline for a public authority to respond to requests made under the Act is 20 working days, although there are some circumstances where this may be extended under the terms of the legislation.

A request for information under the general rights of access must be:

- received in writing
- state the name of the applicant and an address for correspondence
- clearly describe the information requested
- A request can also be made electronically via email.

Exemptions

The rights within the Act may be limited by applying certain exemptions. Several sections of the Act confer an absolute exemption on information. There are 23 exemptions from the rights of access under the Act. These exemptions mark out the limits of the right of access to information under the Act. Further details about applying exemptions can be obtained from the FOI team.

Other sections of the FOI Act direct the CCG to weigh up whether the public interest in maintaining the bar on confirmation/denial or in maintaining the exemption is greater than the public interest in disclosing whether the public authority holds the information, or in disclosing the information at all. In some cases, if an exemption applies the CCG may be obliged to disclose the information if the public interest test outweighs the exemption.

Refusal of requests

NHS St Helens CCG is obliged to disclose information requested under the Act unless an exemption applies to the information requested. If the CCG refuses a request, the applicant should be informed, at the same time as notification of the exemption, of the procedure to follow if the requester is not satisfied. This procedure includes an internal review by the CCG, if the requester is not happy with the findings of the internal review then they should be directed to make a complaint to the ICO. Further details of dealing with FOI refusals should be sought from the FOI Team.

If a request is made for information that is subject to a current piece of work and premature disclosure is not deemed in the public interest, then the Trust can withhold the information temporarily. If withheld, then an indication of when the information will be available should be given.

Release of employee names and details

As a public authority, there is a recognised justification for the disclosure of some employee names and contact details. Board member and other staff members whose name are already published on the CCG's website will be released without seeking additional consent.

Those staff with public facing roles will have work contact details routinely released however, for other staff, consent will normally be sought if release is deemed appropriate. Personal contact details (home address, home telephone number or personal email address) will **never** be released in response to a request under the Act.

Time limits for compliance with requests

The CCG has a statutory obligation to comply with the Freedom of Information Act and has established systems and procedures to ensure that the organisation complies with the Act and to provide the information requested within 20 working days of a request.

Compliance with the 20-day time limit arising from FOI requests is also monitored.

If the CCG chooses to apply an exemption to any information, or it exceeds the appropriate limit for costs of compliance, a notice shall be issued within twenty working days informing the applicant of this decision.

What to do if you receive a request for information

If a member of staff receives a request, it must be passed to the FOI Team immediately. Failure to do this may result in a delay in processing the request and complying with the Law.

All requests should be sent to sthelensccg.foi@nhs.net

Monitoring and Evaluation

The CCG will ensure that monitoring and evaluation of the implementation of FOI takes place on a regular basis. The FOI team will report progress reports to the Finance, Governance & Risk Committee and will include following:

- Number of requests
- Breaches in response times (detailed exception reports)
- Justification of exemptions
- Complaints
- Any requests escalated to the ICO

Network and IT Security Policies

Links to IT Provider policies

IT services are provided to the CCG by St Helens and Knowsley Health Informatics Service (HIS). Their policies are available to the CCG on request or via the Staff Intranet at http://nww.sthelensccg.nhs.uk/governance/policies-and-protocols/:

- Code of Confidentiality
- Mobile Devices Policy
- Remote Access
- Disaster Recovery
- Network Security

Registration Authority Policy and Procedure available on request of via the Staff Intranet at http://nww.sthelensccg.nhs.uk/governance/policies-and-protocols/

Appendix A - Information Governance Management Framework

	Requirement	Detail
Senior Roles within the CCG	**Accountable Officer:** Professor Sarah O'Brien Clinical Accountable Officer	The Clinical Accountable Officer of St Helens CCG has overall accountability and responsibility for Information Governance in the CCG and is required to provide assurance through the Annual Governance Statement that all risks to the organisation, including those relating to information, are effectively managed and mitigated.
	Senior Information Risk Owner and Executive IG Lead: Iain Stoddart Chief Finance Office	The Senior Information Risk Owner (SIRO) is an Executive Director of St Helens CCG Board. The SIRO is expected to understand how the strategic business goals of the CCG may be impacted by information risks. The SIRO will act as an advocate for information risk on the Board and in internal discussions and will provide written advice to the Accountable Officer on the content of their Annual Governance Statement in regard to information risk. The SIRO will provide an essential role in ensuring that identified information security threats are followed up and incidents managed. They will also ensure that the Board and the Accountable Officer are kept up to date on all information risk issues. The role will be supported by the Midlands and Lancashire Commissioning Support Unit Information Governance Team and the Caldicott Guardian, although ownership of the Information Risk Agenda will remain with the SIRO. The SIRO will be supported through a network of Information Asset Owners and Administrators who have been identified and trained throughout the organisation. The SIRO is also appointed to act as the overall Information Governance lead for the CCG and co-ordinate the IG work programme. The Executive IG Lead role has been assigned as Department of Health response to the Caldicott 2 Review contains an expectation that organisations across health and social care strengthen their leadership on information governance. The IG lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG, although the key tasks are likely to be delegated to an Operational IG Lead.
	Caldicott Guardian: Lisa Ellis Chief Nurse	The St Helens CCG Caldicott Guardian has particular responsibility for reflecting patients' interests regarding the use of patient identifiable information and to ensure that the arrangements for the use and sharing of clinical information comply with the Caldicott principles. The Caldicott Guardian will advise on lawful and ethical processing of information and enable information sharing. They will ensure that confidentiality requirements and issues are represented at Board level and within the St Helens CCG's overall governance framework.
	Data Protection Officer Angela Delea Associate Director: Corporate Governance	The Data Protection Officer (DPO) reports to the SIRO. This ensures the DPO can act independently, without a conflict of interest and report direct to the highest management level. The DPO is responsible for ensuring that the CCG and its constituent business areas remain compliant at all times with data protection, privacy & electronic communications regulations, freedom of information act and the environment information regulations. The DPO shall lead on the provision of expert advice to the organisation on all matters concerning the information rights law, compliance, best practice and setting and maintaining standards.
	Information Governance Organisational Lead: Hayley Gidman, Head of Information Governance (Midlands and Lancashire Commissioning Support Unit)	The key purpose of the role is to ensure St Helens CCG successfully achieves the required level of compliance across all requirements of the NHS Digital Information Governance Toolkit. The post holder will support the CCG to ensure the establishment of corporate standards and a consistent CCG wide approach to Information Governance and will be responsible for assuring the implementation of a range of policies, processes, monitoring audits and training and awareness mechanisms to ensure a high level of compliance.

	Information Governance Organisational Lead: Angela Delea Associate Director: Corporate Governance	The key purpose of the role is to ensure St Helens CCG successfully implements a range of policies, processes, monitoring audits and training and awareness mechanisms to ensure a high level of compliance with Information Governance & Information Security. The post holder will ensure the implementation of corporate standards and a consistent organisation wide approach to Information Governance & Information Security.		
Key Policies Policies set out the scope and intent of the organisation in relation to the management of Information Governance.	**Ratification Schedule:**	**[IG Group]**	**[Audit Committee]**	**Board**
	Information Governance Policy	Insert ratification date 25/07/2018	Insert ratification date N/A	Insert ratification date 12/09/18
	Information Governance Handbook	Insert ratification date 25/07/2018	Insert ratification date N/A	Insert ratification date 12/09/18
	Policies are communicated to all staff via the staff website.			
Key Governance Bodies A group, or groups, with appropriate authority should have responsibility for the IG agenda.	**Executive Leadership Team (ELT) Governance Committee**	The ELT Governance Committee is responsible for overseeing day to day Information Governance issues, developing and maintaining policies, standards, procedures and guidance, coordinating and raising awareness of Information Governance in the CCG.		
Resources Details of key staff roles	**Dedicated Information Governance Staff**	Information Governance Business Partners Name: Pippa Joyce Email: pippa.joyce@nhs.net Deputy Head of Information Governance Name: Emma Styles Email: emmastyles@nhs.net Head of Information Governance Name: Hayley Gidman Email: Hayley.gidman@nhs.net		
Governance Framework Details of how responsibility and accountability for IG is cascaded through the organisation.	**Information Asset Owners**	Information Asset Owners are senior individuals involved in running the relevant business. The IAOs role is to: • Understand and address risks to the information assets they 'own'; and • Provide assurance to the SIRO on the security and use of these assets. Information Asset Owners have been nominated across the whole organisation and have received specialist information risk training to allow them to be effective in their role.		
	Information Asset Administrators	The Information Asset Administrators and will: • Ensure that policies and procedures are followed • Recognise potential or actual security incidents • Consult their IAO on incident management • Ensure that information assets registers are accurate and maintained up to date. Information Asset Owners have received specialist information risk training to allow them to be effective in their role.		
	Employment Contracts	All staff and those undertaking work on behalf of the CCG need to be aware that they must meet information governance requirements and it is made clear to them that breaching these requirements, e.g. service user confidentiality, is a serious disciplinary offence. This is supported by the inclusion of clauses within staff contracts both for substantive and temporary staff that cover Information Governance standards and responsibilities with regard to data protection, confidentiality, and information security.		

Structure Chart – Information Governance Management Framework