NHS
Leeds Clinical Commissioning Groups Partnership

INFORMATION GOVERNANCE POLICY AND MANAGEMENT FRAMEWORK

Version:	1.1
Ratified by:	Quality and Performance Committee
Date ratified:	11th January 2018
Name & Title of originator/author:	John Robinson, Senior Information Governance Specialist (eMBED Health Consortium)
Name of responsible committee/individual:	Information Governance Committee
Date issued:	22nd January 2018
Review date:	2019
Target audience:	All staff

Equality Statement

This policy applies to all employees, Governing Body members and members of Leeds Clinical Commissioning Group's Partnership irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership.

A full Equality Impact Assessment is not considered to be necessary as this policy will not have a detrimental impact on a particular group.

Contents

1. INTRODUCTION....4
2. AIMS....4
3. SCOPE....4
4. ORGANISATIONAL ROLES AND ACCOUNTABILITY....5
   - 4.1 Governing Body....5
   - 4.2 Quality and Performance Committee....6
   - 4.3 Information Governance Committee....6
   - 4.4 Senior Information Risk Owner....6
   - 4.5 Caldicott Guardian....7
   - 4.6 Information Asset Owners and Administrators....7
   - 4.7 Head of Governance....7
   - 4.8 Managers....8
   - 4.9 Employees....8
   - 4.10 Third Party Contractors....8
   - 4.11 Clinical Services....8
   - 4.12 Support Services....9
5. Governance Arangements....9
6. Key principles and Procedures....10
   - 6.1 Openess and transparency....10
   - 6.2 Legal compliance....10
   - 6.3 Information Security....11
   - 6.4 Clinical Information Assurance, Quality Assurance and Records....12
7. TRAINING
8. INCIDENT MANAGEMENT....12
9 MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY
10. ASSOCIATED DOCUMENTS....13

11. RELEVANT LEGISLATION 14
12. IMPLEMENTATION AND DISSEMINATION 15
APPENDIX 1: DOCUMENTED ACTION PLAN FOR RAISING STAFF AWARENESS
13. REVIEW 16
APPENDIX 2: INFORMATION GOVERNANCE COMMITTEE TERMS OF REFERENCE 20
APPENDIX 3: INFORMATION GOVERNANCE DECLARATION FORM 23

1. Introduction

The Leeds CCGs recognise the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. The CCGs also recognises the duty of confidentiality owed to patients, families, staff and business partners with regard to all the ways in which it processes, stores, shares and disposes of information.

This overarching Information Governance Policy and Management Framework sets out how Leeds CCGs will meet their information governance obligations and outlines the underlying operational policies and procedures which will enable the CCGs to fulfil their information governance responsibilities.

The policy provides 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.

2. Aims

The aim of this policy is to ensure that all staff understand their obligations with regard to any information which they come into contact with in the course of their work and to provide assurance to The Governing Body that such information is dealt with legally, securely, efficiently and effectively.

The CCG will establish, implement and maintain procedures linked to this policy to ensure compliance with the General Data Protection Regulation (EU) 2016/679 and Data Protection Act, and other related legislation and guidance, contractual responsibilities and to support the assurance standards of the Information Governance Toolkit (Data Security and Protection Toolkit from April 2018).

This policy supports the CCG in its role as a commissioner of health services and will assist in the safe sharing of information with its partner agencies.

3. Scope

This policy must be followed by all staff who work for or on behalf of the CCG including those on temporary or honorary contracts, secondments, volunteers, pool staff, Board members, students, partner CCGs and eMBED Health Consortium staff working on behalf of the CCG. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

This policy and framework covers all aspects of information within the organisation, including (but not limited to):

- Patient/Client/Service User information
- Personnel/Staff information
- Organisational information
- Structured and unstructured record systems - paper and electronic
- Photographic images, digital, text or video recordings including CCTV
- All information systems purchased, developed and managed by/or on behalf of the organisation
- CCG information held on paper, floppy disc, CD, USB/Memory sticks, computers, laptops, tablets, mobile phones and cameras

The processing of all types of information, including (but not limited to):

- Transferring of information – fax, e-mail, post, telephone and removable media such as laptops and memory sticks, etc.
- Sharing of information for clinical, operational or legal reasons
- The storage and retention of information
- The destruction of information

Information governance within an independent contractor's premises is the responsibility of the owner/partners. However, the CCG is committed to supporting independent contractors in their management of information risk and will provide advice, share best practice and provide assistance when appropriate.

The CCG recognises the changes introduced to information management as a result of the Health and Social Care Act 2012 and the Health and Social Care (Safety and Quality) Act 2015 and will work with national bodies and partners to ensure the continuing safe use of information to support services and clinical care.

Failure to adhere to this policy may result in disciplinary action and/or referral to the appropriate regulatory bodies including the police and professional bodies.

4. Organisational Roles and Accountability

Key staff involved in the Information Governance agenda, below those at Executive Team level, will be provided to the CCG through a contract between the CCG and eMBED Health Consortium.

4.1 The Governing Body

The Governing Body is accountable for ensuring that the necessary support and resources are available for the effective implementation of this policy. It has responsibility for the Information Governance Agenda supported by identified senior roles i.e. Caldicott Guardian and SIRO.

4.2 Quality and Performance Committee

The Information Governance agenda will be led by the SIRO supported by staff of eMBED Health Consortium and will report through IG Committee to Quality and Performance Committee.

The IG work programme, and new or significantly amended strategies and policies are escalated to the IG Committee for their consideration and onward approval by Quality and Performance Committee.

4.3 Information Governance Committee

The IG Committee meets on at least a quarter basis and consists of the three SIROs, Caldicott Guardians, eMBED Health Consortium Senior IG Specialist, and appropriate representation. The IG Committee will:

- report to the Quality and Performance Committee
- support the SIROs and Caldicott Guardians in their roles
- monitor information governance performance annually using the Information Governance Toolkit (Data Security and Protection Toolkit from April 2018) (hosted by NHS Digital).
- be responsible for overseeing operational information governance issues
- develop and maintain policies, standards, procedures and guidance
- co-ordinate and monitor the implementation of the information governance strategy, framework and policy across the CCGs
- provide direction in formulating, establishing and promoting IG policies
- ensure that the approach to information handling is communicated to all staff and made available to the public
- ensure that appropriate training is made available to staff and completed as necessary to support their duties
- monitor information handling activities to ensure compliance with the law and guidance

Further information can be found in Appendix 2, which includes the Terms of Reference for the IG Committee.

4.4 Senior Information Risk Owner

The role of the SIRO will be carried out by the Chief Finance Oficer. The SIRO is responsible for ensuring that organisational information risk is properly identified, managed and that appropriate assurance mechanisms exist. The SIRO will:

- understand how the strategic business goals of the CCGs may be impacted by information risks, and how those risks may be managed
- implement and lead the CCGs information governance risk assessment and management processes within the organisation
- providing a focal point for the resolution and/or discussion of IG issues
- own the CCGs Information Security Policy

- undertake training as necessary to ensure they remain effective in their role as SIRO
- manage of the annual IG work programme regarding the IG Service provided by eMBED Health Consortium.

4.5 Caldicott Guardians

The role of the Caldicott Guardians will be carried out by Clinical Directors. The Caldicott Guardians oversee the arrangements for the use and sharing of patient information and will:

- act as the 'conscience' of the CCGs
- represent and champion Information Governance requirements and issues at a senior management level
- facilitate and enable information sharing and advise on options for lawful and ethical processing of information
- ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff
- oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS
- undertake training as necessary to ensure they remain effective in this role

4.6 Information Asset Owners and Administrators

Information Asset Owners (IAO) are senior individuals involved in the running of their respective business functions and are directly accountable to the SIRO. IAOs must provide assurance that information risk is being managed effectively in respect of the information assets they are responsible for and that any new changes introduced to their business processes and systems undergo a privacy impact assessment.

An Information Asset Administrator (IAA) will have delegated responsibility for the operational use of an Asset.

4.7 Head of Corporate Governance

The Head of Corporate Governance will:

- Monitor all requests for information under the Freedom of Information Act by members of the public, and coordinates the responses
- Maintain and publish the organisations Publications Scheme
- Manage Subject Access Requests and requests for information

.

4.8 Managers

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

4.9 Employees

Information Governance compliance is an obligation for all staff. Staff should note that there is confidentiality clause in their contract and that they are expected to participate in induction training, annual refresher training and awareness raising sessions carried out to inform/update staff on information governance issues. Any breach of confidentiality, inappropriate use of health, business or staff records or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract and must be reported to the SIRO and (in the case of health or social care records), the Caldicott Guardian.

All employees are personally responsible for compliance with the law in relation to the General Data Protection Regulation (EU) 2016/679, Data Protection Act 1998 and the Common Law Duty of Confidentiality.

4.10 Third Party Contractors

Contracts with third parties providing services to Leeds CCGs must include appropriate, detailed and explicit requirements regarding confidentiality and information governance to ensure that contractors are aware of their IG obligations. Further guidance is available from the CCGs Provider Contract and Commissioning Information Governance Assurance document.

4.11 Clinical Services

All clinical services commissioned by or on behalf of the CCGs will be required to:

- Have a suitable contract in place to form a joint data controller relationship regarding the information required to effectively monitor commissioned services
- Ensure the services commissioned meet the requirements of the General Data Protection Regulation and Data Protection Act when providing services including, but not limited to, fair processing and up until April 2018 maintaining a registration with the Information Commissioners Office
- Complete the annual Information Governance Toolkit (Data Security and Protection Toolkit from April 2018) as required and undertake an independent audit if requested, to be disclosed to the CCGs in order to provide further assurance they have met expected requirements
- Ensure privacy notices make individuals aware of a CCGs role in commissioning and the personal and sensitive data it may receive to undertake such a role

- Ensure that where any IG incidents occur that they are reported to the CCGs via routes determined within the contract and in accordance with data protection legislation
- Set out expectations regarding providing information in relation to requests for information made under the Freedom of Information Act
- Ensure inclusions regarding Exit Plans are addressed following transfer of services or decommission of service e.g. passing on data/deletion/ retention of data at end of the contract

4.12 Support services

All support services that process information on behalf of the CCGs will be required to:

- Ensure a suitable contract/SLA and or as a minimum a confidentiality agreement is in place to form a Data Controller to Data Processor relationship where Personal or Special Categories of Personal Data is managed on behalf of the CCGs
- Ensure that the services commissioned meet the requirements of the General Data Protection Regulation and Data Protection Act when providing services including, but not limited to, fair processing and up until April 2018 maintaining a registration with the Information Commissioners Office
- Complete the annual Information Governance Toolkit (Data Security and Protection Toolkit from April 2018) (if required) and at the request of the CCGs undertakes a compliance check/audit, in order to provide assurance they have met expected requirements
- Ensure that any new processing is within the remit of the contract or seek written confirmation if there is any ambiguity
- Report any known incidents or risks in relation to the use or management of information owned by the CCGs and in accordance with the General Data Protection Regulation
- Set out expectations regarding providing information in relation to requests for information made under the Freedom of Information Act
- Ensure inclusions regarding Exit Plans are addressed following transfer of services or decommission of service e.g. passing on data/deletion/retention of data at end of the contract

5. Governance Arrangements

The following governance arrangements have been agreed:

- The Health Commissioning and Systems Integration will receive periodic assurance that management and accountability arrangements are adequate and are informed in a timely manner of future changes in the IG agenda by IG updates to the Quality and Performance Committee.
- The CCGs obtain Information Governance Support through a contract with eMBED Health Consortium.

- Responsibility and accountability for Information Governance will be cascaded through the organisation via staff contracts, contracts with third parties, Information Asset Owner arrangements and departmental leads.

6. Key Principles and Procedures

6.1 Openness and Transparency

- The CCGs recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.
- Information will be defined and where appropriate kept confidential underpinning the principles of Caldicott, legislation and guidance.
- Privacy Impact Assessments will be completed where suggested in the respective procedure.
- Information about the organisation will be available to the public in line with the Freedom of Information Act, Environmental Information Regulations and Protection of Freedoms Act unless an exemption applies. The CCGs will establish and maintain a Publication Scheme in line with legislation and guidance from the Information Commissioner. The CCGs will publish approved Privacy Impact Assessments on their website (subject to redaction if applicable) within the Publication Scheme.
- There will be clear procedures and arrangements for handling queries from patients, staff, other agencies and the public concerning personal and organisational information.
- Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.
- Legislation, national and local guidelines will be followed.
- The CCGs will undertake annual assessments and audits (through the Information Governance Toolkit) of its policies, procedures and arrangements for openness.
- Patients will have ready access to information relating to their own health care under the General Data Protection Regulation (EU) 2016/679 and Data Protection Act 1998 using the CCG's Data Protection and Confidentiality Policy and Access to Records Procedure under Data Protection Act 1998 and Access to Health Records Act 1990
- The CCGs will have clear procedures and arrangements for liaison with the press and broadcasting media

6.2 Legal Compliance

- The CCGs regard all identifiable personal information relating to patients as confidential. Compliance with legal and regulatory requirements will be achieved, monitored and maintained.
- The CCGs will undertake or commission annual assessments and audits of its compliance with legal requirements as part of the annual review and submission of the Information Governance Toolkit (Data Security and Protection Toolkit from

April 2018) and in line with changes and developments in legislation and guidance.

- The CCGs regard all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise as set out in the principles of the Human Rights Act and in the public interest
- The CCGs will establish and maintain policies to ensure compliance with the General Data Protection Regulation and Data Protection Act, Freedom of Information Act, Human Rights Act and the common law of confidentiality and associated guidance.
- The CCGs will work with partner NHS bodies and other agencies to establish Information Sharing Protocols to inform the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation Information Governance training will be mandatory for all staff. This will include awareness and understanding of Caldicott principles and confidentiality, information security and data protection. Information Governance will be included in induction training for all new staff with completion of refresher training on an annual basis thereafter. The necessity and frequency of any further training will be Personal Development Review (PDR) based.
- The CCGs will work in collaboration with the Local Counter Fraud Specialists and other related agencies to support their work in detecting and investigating fraudulent activity across the NHS.

6.3 Information Security

- In line with NHS Improvement's 'statement of requirements', the CCGs will appoint a named executive Board member responsible for data and cyber security and also ensure that the Chief Operating Officer confirm an annual 'statement of resilience' to confirm that actions being undertaken to meet the data security requirements.
- The CCGs will establish and maintain policies for the effective and secure management of its information assets and resources
- The CCGs will undertake or commission annual assessments and audits of its information and IT security arrangements as part of the annual review and submission of the Information Governance Toolkit (Data Security and Protection Toolkit from April 2018) and in line with changes and developments in legislation and guidance.
- The CCGs will promote effective confidentiality and information security practice to its staff through policies, procedures and training.
- The CCGs will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
- The CCGs will appoint a Senior Information Risk Owner and assign responsibility to Information Asset Owners to manage information risk.
- The CCGs will use pseudonymisation and anonymisation of personal data where appropriate to further restrict access to confidential information.
- All new projects, processes and systems (including software and hardware) which are introduced must meet confidentiality and data protection requirements. To

enable the organisation to address the privacy concerns a Privacy Impact Assessment (Data Protection Impact Assessment under GDPR) must be used.

6.4 Clinical Information Assurance, Quality Assurance and Records Management

- The CCGs will establish and maintain policies and procedures for information quality assurance and the effective management of records
- The CCGs 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 of, the quality of information within their services
- Wherever possible, information quality should be assured at the point of collection
- The CCGs will promote data quality through policies, procedures, user manual and training.
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The CCGs will establish a Records Management and Information Lifecycle Policy covering all aspects of records management and consistent with the Records Management Code of Practice for Health and Social Care 2016.

7. Training

The CCGs includes Information Governance as part of its mandatory training for all staff annually. All staff are required to complete the Data Security Awareness Level 1 training module via Electronic Staff Record portal.

New staff must review the IG Handbook and sign the Information Governance Declaration before being provided with any access to CCG information assets.

The CCGs have identified other recommended training for staff members whose role has information governance responsibilities and requires further role specific training. Ad hoc training may be completed where an incident investigation requires this. Specific training needs are detailed within the IG Training Strategy.

8. Incident Management

Information Governance and IT related incidents, including cyber security incidents must be reported and managed through the CCGs Incident Management Policy and Serious Incident Policy. An information governance incident of sufficient scale or severity to be classified as a Level 2 Information Governance and Cyber Security Serious Incidents Requiring Investigation will be:

- Notified immediately to the CCG's SIRO and Caldicott Guardian

- Reported to the Department of Health, Information Commissioners Office and other regulators via STEIS and the IGT Incident reporting tool within 72 hours (noting this is a requirement of the General Data Protection Regulation)
- Investigated and reviewed in accordance with the guidance in the HSCIC checklist
- Reported publicly through the CCGs Annual Report and Governance Statement

9. Monitoring Compliance and Effectiveness of the Policy

An assessment of compliance with the requirements in the Information Governance Toolkit (IGT) will be undertaken each year. Annual assessments and proposed action/development plans will be presented to the CCG's Senior Information Risk Owner. The requirements are grouped into the following initiatives:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance

10. Associated Documents

Leeds North CCG will maintain the following key policies to support effective Information Governance:

- Subject Access Request (Access to Health Records) Procedure
- Confidentiality and Data Protection Policy
- Freedom of Information Act and Environmental Regulations Policy
- Information Governance Policy and Management Framework
- Information Governance Strategy
- Information Security Policy
- Records Management and Information Lifecycle Policy

Supplementary to the key policies listed above, Leeds CCGs will also maintain the following policies and guidelines:

- Confidentiality Code of Conduct
- Email Policy
- Internet and Social Media Policy
- Safe Transfer Guidelines and Procedure
- Privacy Impact Assessment Procedure
- Network Security Policy

Details of all the above polices, including where the policy was last approved and the date of last approval are detailed in appendix 1.

Each policy will be subject to an implementation plan:

- All policies will be maintained on the Leeds North CCG Intranet.
- Policies will be incorporated into induction and training sessions as appropriate

11. Relevant Legislation

There are many different standards and legislation that apply to IG and information handling, including, but not limited to:

- Abortion Regulations 1991
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act 1998)
- Access to Medical Records Act 1988
- Audit & Internal Control Act 1987
- Common Law Duty of Confidentiality
- Communications Act 2003
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992
- Coroners and Justice Act 2009
- Crime and Disorder Act 1998
- Data Protection Act 1998
- Data Retention and Investigatory Powers Act 2014
- Digital Economy Act 2017
- Environmental Information Regulations 2004
- Equality Act 2010
- Freedom of Information Act 2000
- General Data Protection Regulation (EU) 2016/679
- Health and Social Care (Safety and Quality) Act 2015
- Health and Social Care Act 2012
- Human Fertilisation and Embryology Act 1990
- Human Rights Act 1998
- Medical Act 1983
- Mental Capacity Act 2005
- NHS Act 2006
- NHS Digital. "FAQs on legal access to personal confidential data." Accessed 16 September 2016. Available from http://digital.nhs.uk/article/3638/Personal-data-access-FAQs.
- NHS Sexually transmitted disease regulations 2000
- Prevention of Terrorism (Temporary Provisions) Act 1989 & Terrorism Act 2000
- Privacy and Electronic Communications Regulations 2003
- Protection of Freedoms Act 2012
- Public Interest Disclosure Act 1998
- Public Records Act 1958
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations 2000)

- Regulations under Health and Safety at Work Act 1974
- Road Traffic Act 1988
- The Children Act 1989 and 2004

12. Implementation and Dissemination

All the Information Governance policies and procedures will be made available in electronic format and will be located on the CCG Intranet. Any updates/new policies/procedures are approved by the Governance Performance and Risk Committee following consideration at the IG Committee and are communicated to staff via the intranet and staff briefings.

Every new member of staff will be directed to the policy pages on the intranet as part of the induction process.

13. Review

This policy will be reviewed every year or in line with changes to relevant legislation or national guidance.

APPENDIX 1: DOCUMENTED ACTION PLAN FOR RAISING STAFF AWARENESS

1) The NHS Digital Information Governance Toolkit (IGT) (Data Security and Protection Toolkit from April 2018) requires organisations providing health and social care services to have a documented action to promote staff awareness of information governance standards, inform staff of their responsibilities and the consequences of misconduct and advise staff their compliance with IG requirements will be checked and monitored

2) Requirement 14.1-133 states Clinical Commissioning Groups (CCGs) are required to have a documented action plan for raising awareness of and compliance with information governance standards and to **inform staff of their responsibilities and the consequences of misconduct**. Staff may be informed through team meetings, awareness sessions or staff briefing materials. *In all cases, 'staff' refers all staff (new and existing), including new starters, locum, temporary, student and contract staff members).*

3) The IGT Requirements listed below, will be incorporated into the CCG's Information Governance work programme for completing IG Toolkit and forms part of the CCG's IG Training Strategy. The relevant IG Toolkit Requirements which require the CCG to promote staff awareness are as follows:

IGT Req	Level	Key messages to be communicated to staff and made available throughout the organisations	Examples of suitable evidence	Delivery Method
14.1-131	2a	IG Policies have been communicated to appropriate staff and made available throughout the organisation	Selection of Policies – Information Governance Policy; Confidentiality and Data Protection Policy; Information Security Policy; Information Lifecycle Management Policy *(incl. Records Management and Information Quality)*	All policies available on the Internet
14.1-133	1c/2a	Guidelines and training materials for staff setting out the CCG's expectations for working practices and behaviours related to information governance (for new and existing staff)	Staff Code of Conduct; Training materials; IG Handbook; Induction Programme for New Starters	Internet Confidentiality Code of Conduct given to all staff
14.1-134	1a/1b/1c/2c	Information Governance Awareness and Mandatory Training for all staff. Additional	Training Needs Analysis to cover mandatory IG Training/additional training for key staff	IGTT e-Learning Tool/ Face to Face

IGT Req	Level	Key messages to be communicated to staff and made available throughout the organisations	Examples of suitable evidence	Delivery Method
		training for staff in key roles	groups/Induction Programme for New Starters/Training materials/documented training programme/Training Records/Test of Comprehension/Reports evidencing numbers of staff trained	
14.1-230	2b	All staff assigned responsibility for co-ordinating and implementing the confidentiality and data protection work programme (Caldicott Function) have been appropriately trained to carry out their role	Training evidence	as above
14.1-231	1b/2a	There is staff guidance on keeping personal information secure, on respecting the confidentiality of service users and on the duty to share information for care purposes.	Documented/IG Handbook/Leaflet /Staff Induction Materials/Review of TNA	Internet Confidentiality Code of Conduct
14.1-232	2a	Guidelines are provided to staff regarding the lawful sharing of confidential personal information	as above	as above
14.1-234	2a/2b	All staff members are aware of their responsibility to support subject access requests and where in the organisation such requests are ultimately handled. Front-line staff to be provided with more detailed guidance about the procedure to follow.	Documented procedure for processing SAR requests/TNA/training attendance lists/staff briefing materials/presentations	Internet SAR policy IGTT e-learning training tool evidence
14.1-235	2a	All staff members with the potential to access confidentiality personal information have been informed that monitoring and auditing of access is being carried out, of the need for compliance with confidentiality and security procedures and the sanctions for failure to comply.	Documented confidentiality audit procedure	Internet/team meetings, staff briefing materials, IG compliance spot checks undertaken
14.1-237	2a	All staff members that are likely to introduce	Privacy Impact Assessment procedure	Internet/team meetings,

IGT Req	Level	Key messages to be communicated to staff and made available throughout the organisations	Examples of suitable evidence	Delivery Method
		new information processes or information assets are effectively informed about the requirement to obtain approval from the IG forum (or equivalent) at the proposal stage of the new process or information asst.		awareness sessions delivered by YHCS, staff briefing materials
14.1-250	1a/2a	Employees are informed of the nature and source of any information stored about them, how it will be used, who it will be disclosed to; and their data protection rights regarding access and sharing of the personal information	The CCG's Website to provide information on how personal information about patients or other service users is stored, used and shared and informs individuals about their rights in relation to that information	Privacy notice on website Confidentiality and Data Protection policy on internet
14.1-340	2b	All staff assigned responsibility Information Security have been appropriately trained to carry out their role	Information Governance Management Framework Policy	Training attendance lists/existing qualifications
14.1-343	2a/2b	Procedure advising Smartcard users of the Terms and Conditions they sign up to upon acceptance of a Smartcard. All NHS Smartcard users, including new, temporary and contract staff members are aware that compliance with the T&Cs of NHS Smartcard usage is monitored and of the procedures for breach and disciplinary measures	RA Plan/Procedure setting out Terms and Conditions of Smartcard usage & documented audits showing processes for monitoring NHS Smartcard usage and compliance with T&Cs; audit report on the outcome of checking that all NHS Smartcard users have electronically signed their T&Cs;	Internet/Confidentiality Code of Conduct/Staff briefing materials and induction materials
14.1-345	2a	The SIRO and all other staff assigned responsibility for coordinating and implementing information risk management have been appropriately trained to carry out their role	TNA/training attendance lists/training materials/existing qualifications or training evaluation records	IGTT e-learning module certificate, face to face sessions
14.1-346	2c	All relevant staff are made aware of business continuity plans and any implications for their role - all staff are aware of their roles and responsibilities	Business Continuity Plans for individual Information Assets	Business Continuity policy on Internet/team meeting notes, staff briefing materials

IGT Req	Level	Key messages to be communicated to staff and made available throughout the organisations	Examples of suitable evidence	Delivery Method
14.1-348	1a/2b	There are documented procedures for mobile working or teleworking that provide guidelines for staff on expected behaviours	Internet and Social Media and Email policies, data handling procedures, safe haven procedures, training materials or other staff guidance	Internet, Confidentiality Code of Conduct
14.1-349	2b	Staff members have been informed of the incident reporting procedures and in particular of their own responsibilities for reporting incidents and near-misses	Documented incident management and report procedures and a template incident reporting form for staff	Internet
14.1-350	2c	Relevant staff members have been effectively informed of the secure transfer and receipt requirement for personal and sensitive information	Internet and Social Media and Email policies, data handling procedures, safe haven procedures, training materials or other staff guidance	Internet
14.1-420	2b	All staff assigned responsibility for Information Quality and Records Management Assurance have been appropriately trained to carry out their role	Information Governance Policy and Management Framework	Training attendance lists, training materials, qualification certificates, or training evaluation records

APPENDIX 2: INFORMATION GOVERNANCE COMMITTEE TERMS OF REFERENCE

Leeds CCGs Information Governance Committee
Terms of Reference

Purpose

The Leeds Information Governance (IG) Committee is a formal city-wide committee forming part of the governance and assurance framework for each of the three Clinical Commissioning Groups (CCGs) in Leeds. These CCGs include Leeds North, Leeds West and Leeds South and East.

The Committee will assist each CCG in ensuring that it manages and uses information securely and safely in compliance with the associated legislation.

An IG Committee is recommended within the national Information Governance Toolkit (IGT) to support and drive the broader IG agenda and provide each CCG Board or Governing Body with the assurance that effective IG best practice mechanisms are in place within the organisation.

The Leeds CCGs IG Committee will ensure that the appropriate policies, procedures and structures are developed and put in place to provide a robust governance framework for information management, thereby ensuring CCG compliance with the national IGT in the following key areas:

- Associated Regulations
- Caldicott Principles
- Confidentiality (including Common Law) and Consent
- Data Protection Act 1998
- Data Quality
- Freedom of Information Act 2000
- General Data Protection Regulations 2016
- Information Security
- Information Sharing
- Privacy and Electronic Communications Regulations 2003
- Records Management

Objectives

The main objectives of the Leeds IG Committee will be to:

- Ensure that the CCGs satisfy statutory and NHS requirements and standards concerning information governance.
- Recommend effective policies and management arrangements covering all aspects of IG in line with the CCGs overarching IG Policy and Strategy, for approval.
- Ensure that the CCGs undertakes regular assessments and audits of its IG policies and arrangements.

- Establish an annual IG action plan, secure the necessary implementation resources, and monitor the implementation of that plan.
- Define clear lines of accountability for IG policy, practice and implementation.
- Support the Caldicott Guardian and Senior Information Risk Owner.
- Identify and evaluate areas of risk, set priorities and, where appropriate, undertake or recommend remedial action in relation to information processing issues e.g. breaches of confidentiality or security, audit or data quality reports.
- Review any information assets spanning over more than an individual CCG.
- Advise on the introduction of changes to processes and systems within the CCGs or shared with partner agencies, to ensure the safe and secure processing of personal information.
- Monitor compliance with Information Sharing Protocols.
- Promote education and training programmes for staff in order to support improvements in the CCGs information processing practice and culture.
- To ensure staff receive up to date guidance on confidentiality and information sharing.
- Liaise with other CCGs committees, working groups and boards in order to promote IG and resolve any issues.
- As part of the CCGs delegated responsibility from NHS England, to support General Practitioners with advice to enable them to complete their IGT submissions.
- Establish, implement and monitor the commissioned IG support services delivered under contract or Service Level Agreement and agreed annual work programme.
- Monitor compliance with each CCGs obligations under the Freedom of Information Act.
- Discuss and review detailed IG queries, especially where subsequent advice may affect more than one CCG.
- Review Privacy Impact Assessments which involve more than a single CCG.
- Review any overseas data flows.

Frequency of meetings

The Group will meet a minimum of four times a year. Meeting minutes will be taken.

Reporting

The Leeds CCGs partnership IG Committee will report to the CCGs Quality and Performance Committee

This will generally be by means of the following:

- A copy of the IG Committee minutes
- An IG summary that covers any IG matters that need to be brought to the attention of the relevant assurance committee

Membership of the Group

The core membership of this group will include:

- Director of Informatics – Chair
- IG Manager/Specialist
- Senior Information Risk Owner (SIRO)
- Caldicott Guardian
- An Information Asset Owner (IAO)

Others may attend when agenda requires.

Quoracy

The IG Committee will be quorate when the Chair, a SIRO and/or Caldicott Guardian and one representative per CCG from the core membership are present. The CCG representative may include the Chair, SIRO or Caldicott Guardian.

The Chair may within their city-wide role be delegated to fulfil the above representative requirement for one CCG only.

Accountability

The Leeds IG Committee will be accountable to Leeds CCGs Quality and Performance Committee.

APPENDIX 3: INFORMATION GOVERNANCE DECLARATION FORM

Information Governance Declaration Form

I confirm that I have received the Information Governance and Data Security User Handbook and understand that it is my responsibility to read and understand it and to raise any queries or concerns with my line manager or directly with the Information Governance team (EMBED.infogov@nhs.net).

This booklet has been developed to ensure that users are compliant with, but not limited to the General Data Protection Regulation (EU) 2016/679, Data Protection Act 1998, Freedom of Information Act 2000, Human Rights Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patent Act 1988, ISO27001 and the Caldicott principles.

It is important to remember that **you** are accountable for your computer login and that all activity is auditable. Monitoring of email and internet activity is also carried out. It is **your** responsibility to ensure that only you know your password and that if you leave your PC logged in and unattended you must lock your PC (Press Ctrl+Alt+ Del) to stop any unauthorised use of your PC.

If you choose to make a note of any login/IDs and/or passwords that you are using, lock them away in a secure place. Keep all passwords secure and **do not** share them with anyone.

You should be aware that inappropriate use, including any violation of this policy may result in the withdrawal of the facility and may result in prosecution and/or disciplinary action, including dismissal, in accordance with the CCG's disciplinary procedures.

Signed:	
Name (Please PRINT):	
Date:	
Job Title:	
Team:	
Email:	

When signed this declaration will be held on your personal file