Information Governance Framework and Strategy

October 2019

Important: This document can only be considered valid when viewed on the CCG's website.

If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

If you need this document in a different format or language (e.g. large print, Braille, audio or easy read), please contact us on 01482 344700, or email HULLCCG.contactus@nhs.net, or write to: NHS Hull Clinical Commissioning Group, 2nd Floor, Wilberforce Court, Alfred Gelder Street, Hull HU1 1UY.

Name of Policy:	Information Governance Framework and Strategy
Date Issued:	November 2019
Date to be reviewed:	2 years from approval date

Policy Title:	**Information Governance Framework and Strategy**	
Supersedes: (Please List)	Information Governance Framework and Strategy v1.1 Information Governance Framework and Strategy v1.2 Information Governance Framework and Strategy v1.4	
Description of Amendment(s):	Annual review as required by IG Toolkit TOR of Information Governance Group Updated Addition of Sustainability & Bribery Act Sections Organisational IG Structure defined Incident Reporting section updated and flow chart added Reformatting under headings and numbered sections	
This policy will impact on:	All Staff	
Policy Area:	Data Protection	
Version No:	2.0	
Author:	Information Governance Team	
Effective Date:	November 2019	
Review Date:	2 years from approval	
Equality Impact Assessment Date:	October 2019	
APPROVAL RECORD		**Date:**
	Integrated Audit and Governance Committee	November 2019
Consultation:	Information Governance Steering Group Members	October 2019
	Relevant Others / Deputy Heads	October 2019

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Website
1.0	Barry Jackson	First draft for comments	NR	N/A
1.1	Barry Jackson	Approved version	N/A	N/A
1.2	Helen Sanderson	Amendments to reflect HSCIC Guidance and Caldicott 2	N/A	N/A
1.3	Kathleen Allen	IGG TOR Updated Policy formatting updated Addition of Sustainability Section Addition of Bribery Act Organisational IG Structure detailed More Guidance on Incident Reporting including flow chart	N/A	09 March 2017
2.0	Hayley Gillingwater	Removal of IG Toolkit references – replaced with DSPT. Updates to handling confidential information. Updates to incident reporting. Updates to training Updates to principles. Updated TORs. Addition of Data Protection Officer responsibilities.	Integrated Audit and Governance Committee – 15 November 2019	November 2019

CONTENTS

1. INTRODUCTION

The purpose of this framework is to describe the management arrangements that will deliver Information Governance (IG) assurance within Hull Clinical Commissioning Group (afterwards referred to as HULLCCG). Information Governance is a framework that enables the organisation to establish good practice around the handling of information, promote a culture of awareness and improvement and comply with legislation and other mandatory standards.

Information Governance is about setting a high standard for the handling of information and giving organisations the tools to achieve that standard. The ultimate aim is to demonstrate that an organisation can be trusted to maintain the confidentiality and security of personal information, by helping individuals to practice good information governance and to be consistent in the way they handle personal and corporate information.

2. SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff, and others undertaking work on behalf of the CCG.

3. POLICY PURPOSE AND AIMS

Information Governance Strategy

The development of a fixed IG Framework will support an IG Strategy that will develop over time with the current version published at Annex A.

National Context

The NHS Information Governance Assurance Programme (IGAP) was established in February 2008 in response to the Cabinet Office Data Handling review. The Prime Minister commissioned the review following the high-profile data losses in 2007. IGAP developed a number of principles to support and strengthen the existing Information Governance agenda.
The principles are:

- All NHS organisations should be part of the same Information Governance Assurance Framework (IGAF)
- Information Governance should be as much as possible integrated into the broader governance of an organisation, and regarded as being as important as financial and clinical governance in organisational culture
- The Framework will provide assurance to the several audiences interested in the safe custody and use of sensitive personal information in healthcare. This involves greater transparency in organisational business processes around Information Governance
- IGAF to be built on the strong foundations of the existing Information Governance agenda and is the mechanism by which:
    - IG policies and standards are set
    - Regulators can check an organisation's compliance
    - An organisation can be performance managed

The purpose of this local framework is to set out an overall strategy and promote a culture of good practice around the processing of information and use of information systems. That is, to ensure that information is handled to ethical and quality standards in a secure and confidential manner. The organisation requires all employees to comply with the Policies, Procedures and Guidelines which are in place to implement this framework with the aim of ensuring that HULLCCG maintains high standards of IG.

Data Security and Protection Toolkit (DSPT)

The Data Security and Protection Toolkit (DSPT) is an online tool that enables organisations to measure their performance against the information governance requirements and compliance with the toolkit provides assurance that organisations have established good practice around the handling of information, are actively promoting a culture of awareness and improvement to comply with legislation and other mandatory standards.

Completion of the DSPT is mandatory for all organisations connected to N3 the proprietary NHS computer network, for organisations using NHS Mail and providing NHS services. All organisations are required to complete the toolkit to a satisfactory level. Annual plans will be developed year on year from the DSPT to achieve the required standard. As the DSPT is a publically available assessment the scores of partner organisations will be used to assess their suitability to share information and to conduct business with.

Information Security

With the increasing use of electronic data and ways of working which rely on the use of electronic information and communication systems to deliver services there is a need for professional advice and guidance on their use as well as the need to ensure that they are maintained and operated to the required standards in a safe and secure environment.

Data Protection Act (DPA)

The Data Protection) incorporating the requirements of the General Data Protection Regulation (GDPR) is the most fundamental piece of legislation that underpins Information Governance. HULLCCG are registered with the Information Commissioners Office and will fully comply with all legal requirements of the Act. A process will be adopted to ensure that a review of all of new systems is carried out and where requirements such as the need for a Data Protection Impact Assessments (DPIA) are highlighted these will be completed.

The Principles relating to the processing of personal data are detailed at Annex B.

Caldicott Principles and Requirements

The original Caldicott Report on the Review of Patient-Identifiable Information 1997 and the subsequent Report of the Caldicott2 Review - Information: To share or not

to share? The Information Governance Review 2013. These two reports have identified specific principles that are considered essential practice for the appropriate sharing and security of Patient Information.

Government Response to the Report of the Caldicott 2 Report acknowledges the findings of this and promotes that everyone should understand how to protect and, where appropriate, share information about the people they care for, either directly or indirectly. The Caldicott Principles are detailed at Annex C.

This is further supported by the Everyone Counts: Planning for Patients 2014/15 to 2018/19 by detailing practical applications for information sharing, these are detailed at Annex D.

Handling Confidential Information

When handling confidential information and especially where an individual can be identified from the information to be processed, the CCG must ensure that it has determined and documented a legal basis for processing that information.
In addition it must ensure that arrangements are in place to ensure:

- Ensuring data subjects are appropriately informed of all uses of their information
- The security of that information at all points of its lifecycle.
- Recognising and recording objections to the handling of confidential information and where circumstances under which an objection cannot be upheld.
- Ensuring that where objections are received where the proposed uses are not required by law the CCG should ensure they act in accordance with that objection.
- Implement procedures for recognising and responding to individuals requests for access to their personal information.
- Ensure appropriate information sharing arrangements are in place for the purposes of direct care.
- Ensure appropriate data processing agreements are in place to collect or obtain information for management purposes.
- Ensure staff are appropriately trained to handle confidential information
- Ensure staff are aware of and follow data breach reporting processes

The HSCIC issued two guidance documents in respect of appropriate information handling and confidentiality of that information:

1. **Code of practice on confidential information**: This code of practice describes good practice for organisations handling confidential information concerning, or connected with, the provision of health services or adult social care.
2. **A guide to confidentiality in health and social care**: A for those involved in the direct care of a patient on the appropriate handling of confidential information.

Risk Management

The ability to apply good risk management principles to IG is fundamental and all organisations will apply them through organisational policies. The IG Team will be responsible for completion of the risk assessments for any IG related issue, and have a specific remit to risk assess new technologies and recommend controls where

necessary.

Risk assessment will also be included as part of the Information Asset Owners role. Any information flows from or into identified information assets will be risk assessed and the results reported to the CCG SIRO for risk mitigation, acceptance or transfer.

Awareness and Advice

The IG Team will provide advice on any IG related issue. They will work with the HULLCCG IG Lead to produce newsletters and staff e-mails to provide information and updates on IG issues.

Incident Management

Incident Reporting

Information Governance and IT related incidents, including cyber security incidents (including but not limited to, physical destruction or damage to the organisation's computer systems, loss of systems availability and the theft, disclosure or modification of information due to intentional or accidental unauthorised actions) must be reported and managed through the CCG's Incident Policy. The IG Team will have an active involvement in all IG related incidents and IG related service desk calls to ensure compliance with IG principles. Significant issues will be subject to full investigation and reporting action via the DSPT where appropriate. Incidents relating to personal information will be highlighted to the Caldicott Guardian whilst those of a more technical nature and/or where serious risks are involved will be reported to the SIRO. Please see Incident Reporting Flow Chart attached at Annex F

Under GDPR, where a data breach is likely to result in a risk to the rights and freedoms of the individual, incidents must be reported to the Information Commissioners Office within 72 hours.

An information governance incident of sufficient scale or severity will be:

- Notified immediately to the CCG's SIRO and Caldicott Guardian
- Reported via the Data Security & Protection Toolkit
- Reported to the Department of Health, Information Commissioners Office and other regulators via STEIS and the HSCIC Incident reporting tool
- Investigated and reviewed in accordance with the guidance in the HSCIC checklist
- Reported publicly through the CCGs Annual Report and Governance Statement

Incident Investigation

The IG Team will support the investigation of all IG issues reported. This may include, but is not limited to, breaches of policy, breaches of confidentiality and issues related to IT Security. The IG Team will assist with the procedural processes to ensure that investigations of incidents will be carried out in a way that ensures the preservation of evidence and in a manner that enables both legal and disciplinary action to be taken if necessary.

Organisational Structure for IG Reporting and Assurance

The Information Governance Group has been established to support and drive the broader information governance agenda and provide the Integrated Audit and Governance Committee and the Governing Body with the assurance that effective information governance best practice mechanisms are in place within the organisation.

The Group will meets regularly and membership includes the SIRO, Data Protection Officer and a representative of the provided IG service. Other staff may be invited to attend where the subject topics require their input or advice See Annex E for the Terms of Reference for this group. The Information Governance Group will report to the Integrated Audit and Governance Committee (IAGC) through action notes and will ensure the SIRO and/or Caldicott Guardian briefed on any significant issues. The Governing Body retains overall responsibility and accountability for all aspects of Information Governance.

4. IMPACT ANALYSIS

This Policy forms part of the CCG's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

As part of its development this Policy and its impact on equality has been analysed and no detriment identified.

Bribery Act 2010

NHS Hull Clinical Commissioning Group has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from The Bribery Act 2010.

The Bribery Act 2010 makes it a criminal offence to bribe or be bribed by another person by offering or requesting a financial or other advantage as a reward or incentive to perform a relevant function or activity improperly performed. The penalties for any breaches of the Act are potentially severe. There is no upper limit on the level of fines that can be imposed and an individual convicted of an offence can face a prison sentence of up to 10 years.

For further information see http://www.justice.gov.uk/guidance/docs/bribery-act-2010-quick-start-guide.pdf.

If you require assistance in determining the implications of the Bribery Act please contact the Local Counter Fraud Specialist on telephone number 01482 866800 or email at nikki.cooper1@nhs.net.

Due consideration has been given to the Bribery Act 2010 in the review, of this policy document and no specific risks were identified.

5. NHS CONSTITUTION

5.1 The CCG is committed to:

Eliminating discrimination and promoting equality and diversity in its Policies, Procedures and Guidelines and by designing and implementing services, policies and measures that meet the diverse needs of its population and workforce, ensuring that no individual or group is disadvantage

6. ROLES / RESPONSIBILITIES / DUTIES

6.1 Caldicott Guardian

The Caldicott Guardian for HULLCCG is the Director of Quality and Clinical Governance/Executive Nurse.

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Guardian plays a key role in ensuring that NHS, Councils with Social Services Responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information.

Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information. The Caldicott Guardian also has a strategic role, which involves representing and championing Information Governance requirements and issues at Board or management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

6.2 Senior Information Risk Owner (SIRO)

The SIRO for HULLCCG is the Chief Finance Officer.

The Senior Information Risk Owner (SIRO) is an Executive Director or Senior Management Board Member 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 Accounting Officer on the content of the Organisation’s Annual Governance Statement in regard to information risk.

The SIRO must understand how the strategic business goals of the Organisation and how other organisations’ business goals may be impacted by information risks, and how those risks may be managed. The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the Organisation and advises the Board on the effectiveness of information risk management across the Organisation.

6.3 Information Governance Lead

The Information Governance Lead for HULLCCG is the Chief Finance Officer
The IG Lead works with the IG Specialist to ensure systems are developed and implemented. The IG Lead is responsible for the co-ordination of the implementation within the CCG. The IG lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG within the CCG. This role includes but is not limited to:-

- developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, e.g. an overarching high level strategy document supported by corporate and/or directorate policies and procedures;
- ensuring that there is top level awareness and support for IG resourcing and implementation of improvements;
- providing direction in formulating, establishing and promoting IG policies;
- establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives;
- ensuring annual assessments and audits of IG policies(were required) and arrangements are carried out, documented and reported;
- ensuring that the approach to information handling is communicated to all staff and made available to the public;
- ensuring that appropriate training is made available to staff and completed as necessary to support their duties and for NHS organisations;
- liaising with other committees, working groups and programme boards in order to promote and integrate IG standards;
- monitoring information handling activities to ensure compliance with law and guidance; and
- providing a focal point for the resolution and/or discussion of IG issues.

6.4 Data Protection Officer

The Data Protection Officer works with the IG Lead to ensure systems and projects are safely developed and implemented. The DPO reports to an Associate Director or Senior Management Board member. The tasks of the DPO, as listed in Article 39 of the GDPR are:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
- to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- to cooperate with the supervisory authority;
- to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

6.5 Managers

Managers are responsible for ensuring that their staff, both permanent and temporary, are aware of:

- all information security policies and guidance and their responsibility to comply with them;
- their personal responsibilities for information security;
- where to access advice on matters relating to security and confidentiality; and
- the security of their physical environments where information is processed or stored.

6.6 All staff

Individual employees have a responsibility to ensure they are aware of all information security policies and guidance and comply with them. Staff must be aware of their personal responsibility for the security and confidentiality of information which they use. Staff are responsible for reporting any possible or potential issues whereby a breach of security may occur.

7. IMPLEMENTATION

The policy will be disseminated by being made available on the website and highlighted to staff through newsletters, team briefings and by managers.

'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.

8. TRAINING AND AWARENESS

In accordance with the requirement to achieve a satisfactory Level in the Data Security and Protection Toolkit all staff must complete an Induction session when they first start employment which will include Information Governance. In subsequent years all staff are required to complete further Information Governance (Data Security & Awareness) training including any training specific to their role and responsibilities. Data Security & Awareness training is mandatory and will include awareness and understanding of Caldicott principles and confidentiality, information security and data protection. E-learning products are provided for the training via the eLearning for Health website and ESR.

An Information Governance Handbook and an Information Asset Owners Handbook are available for all staff to ensure that they are fully aware of their responsibilities.

Staff awareness of IG will also be assessed by questions in the Annual Staff survey in order to provide assurance that the training is effective.

9. MONITORING AND EFFECTIVENESS

The effectiveness of this Policy will be monitored by the SIRO.

10. POLICY REVIEW

This Policy will be reviewed within 2 years from the date of implementation. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

11. REFERENCES

- Data Protection Act 2018
- The General Data Protection Regulation (GDPR)
- Human Rights Act 1998 (Specifically Article 8)
- NHS Information Governance: Guidance on Legal and Professional Obligations.
- Report on the Review of Patient-Identifiable Information 1997 (Caldicott Report)
- Report of the Caldicott2 Review - Information: To share or not to share? The Information Governance Review 2013
- Government Response to Report of the Caldicott2 Review 2013.
- National Data Guardian for Health and Care: Review of Data Security, Consent and Opt-Outs
- NHS England: Everyone Counts: Planning for Patients 2014/15 to 2018/19.
- HSCIC: A guide to confidentiality in health and social care: Treating confidential information with respect - September 2013
- HSCIC: A guide to confidentiality in health and social care: references - September 2013
- National Information Board and DH: Personalised Health and Care 2020
- NHS England: NHS Standard Contract
- Information Commissioner: Data Sharing Code of Practice
- Information Commissioner: Privacy Impact Assessment Code of Practice

12. ASSOCIATED DOCUMENTATION

The Information Governance Framework and Strategy are supported by a range of detailed policies and procedures. These include but are not limited to:

- Data Protection and Confidentiality Policy
- Confidentiality: Code of Conduct Policy
- Records Management Policy
- Safe Haven Policy
- Mobile Working Policy
- Information Security Policy
- Business Continuity and Strategy Policy
- Confidentiality Audit Policy
- Subject Access Request Policy

- Acceptable Computer Use Policy
- Email Policy
- Information Governance Handbook
- IAO role and responsibilities/Handbook
- Data Protection Impact Assessment Procedure
- Data Protection by Design and Default Procedure

Annex A

HULL CCG INFORMATION GOVERNANCE STRATEGY 2019 to 20

1. The IG Strategy of HULLCCG will be based upon a vision of a long term delivery of clear open principles to ensure that:

   1.1. The CCG complies with all statutory requirements

   1.2. The CCG has an information governance strategy that supports the achievement of corporate objectives

   1.3. The CCG can demonstrate an effective framework for managing information governance assurance

   1.4. Staff are aware of their responsibilities and the importance of information governance

   1.5. Information governance becomes a systematic, efficient and effective part of business as usual for the organisation

   1.6. Information governance is integrated into the change control process

   1.7. That there are effective methods for seeking assurance across the organisation and with its key partners

   1.8. That the organisation can demonstrate that the information governance arrangements of organisations it commissions services from across healthcare and commissioning support are adequat

Annex B

GDPR Principles relating to processing of personal data

1. Personal data shall be:

    1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

    (a) at least one of the conditions in Article 6 of the GDPR is met, and

    (b) in the case of sensitive personal data, at least one of the conditions in Article 9 of the GDPR or Schedule 1 of the DPA 18 is also met.

    2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

    3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

    4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

    5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

    6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

    7. Personal data shall be processed in accordance with the rights of data subjects under this Act.

    8. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

    9. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Annex C

Caldicott Principles

1. 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.

2. 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).

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

Annex D

Everyone Counts: Planning for Patients 2014/15 -2018/19

This document sets out the NHS England vision with regards to the provision and outcomes of high quality care for all, now and for future generations. One of the six national conditions focuses in on 'Better data sharing between health and social care, based on the NHS number' and that local organisations should 'ensure they have the appropriate Information Governance controls in place for information sharing in line with Caldicott 2, and if not, when they plan for it to be in place.'

The requirements of the above document are as follows:

The CCG should where required

1. Confirm that they are using the NHS Number as the primary identifier for health and care services, and if they are not, when they plan to;
2. Confirm that they are pursuing open APIs (ie. systems that speak to each other); and
3. Ensure they have the appropriate Information Governance controls in place for information sharing in line with Caldicott 2, and if not, when they plan for it to be in place.

NHS England has already produced guidance that relates to both of these areas. (It is recognised that progress on this issue will require the resolution of some Information Governance issues by DH).

ANNEX E

INFORMATION GOVERNANCE STEERING GROUP
TERMS OF REFERENCE

1. PURPOSE

1.1 NHS Hull Clinical Commissioning Group (CCG) has established an Information Governance Steering Group (IGSG). The purpose of the group is to oversee and drive the broader Information Governance Agenda, the implementation of the CCG Information Governance Framework, including identifying lines of accountability and to ensure that information governance practices and procedures are embedded throughout the CCG.

1.2 To provide the Integrated Audit and Governance Committee (IAGC) with the assurance that effective information governance best practice mechanisms and control are in place within the organisation.

1.3 Links and interdependencies

The IGSG will provide assurances, as appropriate, to the IAGC on the matters set out in these Terms of Reference.

2. ACCOUNTABILITY

The IGSG is accountable to the IAGC and is authorised to:

- Investigate any activity within its terms of reference.
- Seek any information it requires from any employee and all employees are directed to co-operate with any request made by the Group. This remit extends to those working on behalf of the CCG.
- Co-ordinate and implement activities in line with these terms of reference, as part of the Information Governance work programme, which shall be signed off by the IAGC.

3. AUTHORITY

3.1 The Group is authorised to investigate any activity within its Terms of Reference. It may seek any information it requires from employees and all employees are directed to co-operate with any request made by the Group.

3.2 The Group is authorised and may seek independent assurance or other expert advice, as necessary, in order to meets its objectives.

4. REPORTING ARRANGEMENTS

4.1 Action notes will be kept and submitted to the IAGC circulated by the Senior Information Governance Specialist.

4.2 The Group will set out an annual workplan to provide assurance on the achievement of its objectives.

4.3 Disclosure/Freedom of Information Act (FOI)
The senior officer with responsibility for corporate governance will be responsible for ensuring that FOI requirements are met whilst confidentiality and information security are maintained as necessary.

4.4 Standards of Business Conduct/Conflict of Interest
All group members must adhere to the CCG's Constitution and Standards of Business Conduct / Conflicts of Interest policies, together with NHS England statutory guidance on managing conflicts of interest.

5. MEMBERSHIP

5.1 The Membership of the Group is listed at Appendix 1.

5.2 Attendance will be monitored throughout the year and any concerns raised with the Chair and relevant Member.

6. APPOINTMENT OF CHAIR

6.1 The Group will be chaired by the Chief Finance Officer (Senior Information Risk Owner).

7. QUORACY

7.1 The quorum for meetings shall be four members including either the Chair or Deputy Chair.

7.2 If a quorum has not been reached, then the meeting may proceed if those attending agree but the notes should indicate this and no decisions may be taken by the non-quorate meeting of the Group.

8. ATTENDANCE

8.1 The Chair of the Group may invite other officers of the CCG, to attend the group, as appropriate.

9. MEETINGS

9.1 The Group shall meet quarterly and on other such occasions as agreed by the Chair.

9.2 The Senior Information Governance Specialist is responsible for the production of the agenda and the action notes of the meeting and the collation and distribution of papers.

9.3 Meetings shall be administered in accordance with the CCG's Constitution, Standing Orders and other relevant frameworks.

10. CONFIDENTIALITY

The Group will conduct its business in accordance with the codes of conduct set out within the CCG Constitution. All attendees will adhere to established standards of business confidentiality.

11. REMIT

Specific Responsibilities are as follows:

- Receive advice and updates on the adoption and implementation of national information governance legislation, standards and guidance covering the following areas:
    - Data Protection and Privacy (including the GDPR whilst applicable to the UK);
    - Freedom of Information Act, Access to Information and Publication of CCG Data;
    - Information and Data Security;
    - Records Management;
    - Data Sharing and Joint Working:
- Develop with NHS Digital Data Sharing Agreements/Data Processing Contracts;
- Ensure that local operational leads are assigned for specific areas of the information governance agenda as appropriate, who will be responsible for providing evidence to support the tool kit scores in their designated area(s);
- Monitor compliance of statutory and mandatory training in respect of Data Awareness and Security Training;
- Monitor implementation of IG requirements within Contracting Processes;
- Monitor the completion of Data Protection Impact Assessments for new projects and services and actions required from the risk assessments;
- Monitor the Information Asset Register, Data Flow Mapping and risk assessments;
- Receive and action the Information Governance work plan;
- Receive reports of information governance incidents and take forward lessons learned resulting from the investigation of those incidents;
- Approve Information Governance policies and procedures;
- Ensure that the Organisation's approach to information handling is communicated to all staff and relevant others;
- To prepare the annual Information Governance assessment for sign off by the IAGC;
- Prepare update reports for IAGC Committee;
- Provide regular bulletins to all staff on IG related topics;

12 REVIEW OF THE TERMS OF REFERENCE

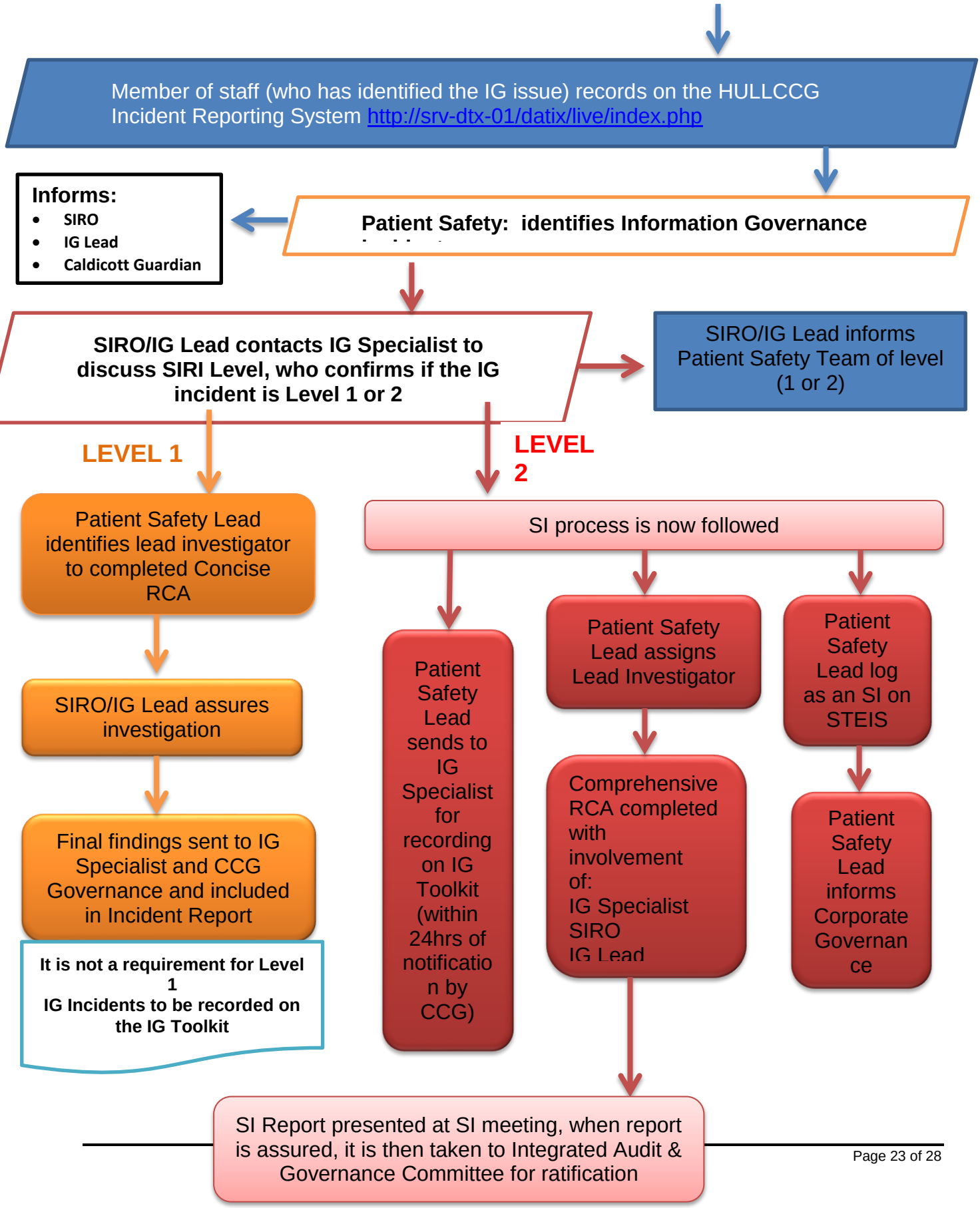
12.1 The Terms of Reference will be reviewed not less than annually and submitted to the IAGC for approval as necessary.

MEMBERSHIP

Membership of the group shall be:

Members
Chief Finance Officer (Senior Information Risk Owner (Chair)
Associate Director of Corporate Affairs (Deputy Chair)
Associate Director of Communications and Engagement
Associate Director of IT or Deputy
Corporate Affairs Manager
Data Protection Officer
Deputy Director of Commissioning
Senior Quality Representative
Head of Performance and Programme Delivery
Senior Information Governance Specialist

Information Governance Incident Reporting Flow Chart Annex F



APPENDICES

Please refer to the EIA Overview & Navigation Guidelines located in *Y:\HULLCCG\Corporate Templates and Forms\Equality and Diversity Information* before completing your EIA)

HR / Corporate Policy Equality Impact Analysis:	
Policy / Project / Function:	Information Governance Framework & Strategy
Date of Analysis:	11/10/2019
Completed by: **(Name and Department)**	Hayley Gillingwater Senior Information Governance Specialist
What are the aims and intended effects of this policy, project or function?	The purpose of this framework is to describe the management arrangements that will deliver Information Governance (IG) assurance within Hull Clinical Commissioning Group.
Are there any significant changes to previous policy likely to have an impact on staff / other stakeholder groups?	No significant changes – Removal of IG Toolkit references – replaced with DSPT. Updates to handling confidential information. Updates to incident reporting. Updates to training Updates to principles. Updated TORs.
Please list any other policies that are related to or referred to as part of this analysis	N/A
Who will the policy, project or function affect?	Staff employed by Hull CCG
What engagement / consultation has been done, or is planned for this policy and the equality impact assessment?	Consultation will take place with Information Governance staff at the Information Governance Steering Group and relevant others.

Promoting Inclusivity and Hull CCG's Equality Objectives. How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation? How does the policy promote our equality objectives: 1. Ensure patients and public have improved access to information and minimise communications barriers 2. To ensure and provide evidence that equality is consciously considered in all commissioning activities and ownership of this is part of everyone's day-to-day job 3. Recruit and maintain a well-supported, skilled workforce, which is representative of the population we serve 4. Ensure the that NHS Hull Clinical Commissioning Group is welcoming and inclusive to people from all backgrounds and with a range of access needs	The policy does not directly promote inclusivity but provides a framework for delivering Information Governance assurance within the CCG.

Equality Data	
Is any Equality Data available relating to the use or implementation of this policy, project or function? Equality data is internal or external information that may indicate how the activity being analysed can affect different groups of people who share the nine *Protected Characteristics* – referred to hereafter as *'Equality Groups'.* Examples of *Equality Data* include: (this list is not definitive) 1: Recruitment data, e.g. applications compared to the population profile, application success rates 2: Complaints by groups who share /	Yes ☐ No x Where you have answered yes, please incorporate this data when performing the *Equality Impact Assessment Test* (the next section of this document). If you answered No, what information will you use to assess impact? **Please note that due to the small number of staff employed by the CCG, data with returns small enough to identity individuals cannot be published. However, the data should still be analysed as part of the EIA process, and where it is possible to identify trends or issues, these should be recorded in the EIA.**

represent protected characteristics 4: Grievances or decisions upheld and dismissed by protected characteristic group 5: Insight gained through engagement	

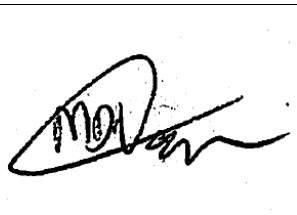
Assessing Impact				
Is this policy (or the implementation of this policy) likely to have a particular impact on any of the protected characteristic groups? (Based on analysis of the data / insights gathered through engagement, or your knowledge of the substance of this policy)				
Protected Characteristic:	**Neutral Impact:**	**Positive Impact:**	**Negative Impact:**	**Evidence of impact and, if applicable, justification where a *Genuine Determining Reason*[1] exists (see footnote below – seek further advice in this case)**
It is anticipated that these guidelines will have a positive impact as they support policy writers to complete meaningful EIAs, by providing this template and a range of potential issues to consider across the protected characteristics below. There may of course be other issues relevant to your policy, not listed below, and some of the issues listed below may not be relevant to your policy.				
Gender	x			This policy applies to all staff regardless of gender.
Age	x			This policy applies to all staff regardless of age.
Race / ethnicity / nationality	x			This policy applies to all staff regardless of race, ethnicity or nationality.
Disability	x			This policy applies to all staff regardless of disability.
Religion or Belief	x			This policy applies to all staff regardless of religion or belief.
Sexual Orientation	x			This policy applies to all staff regardless of sexual orientation.
Pregnancy and Maternity	x			This policy applies to all staff regardless of pregnancy or maternity.

1. [1] *The action is proportionate to the legitimate aims of the organisation (please seek further advice)*

Transgender / Gender reassignment	x			This policy applies to all staff regardless of transgender/ gender reassignment.
Marriage or civil partnership	x			This policy applies to all staff regardless of marriage or civil partnership.

Action Planning:				
As a result of performing this analysis, what actions are proposed to remove or reduce any risks of adverse impact or strengthen the promotion of equality?				
Identified Risk:	**Recommended Actions:**	**Responsible Lead:**	**Completion Date:**	**Review Date:**
As the policy is written in English there is a potential impact on employees whose first language is not English and therefore may struggle reading the policy.	The CCGs internal 'portal' and external website signpost individuals to alternative formats such as large print, braille or another language	CCG Communications	Updating of this facility is ongoing	2 years from approval date.

Sign-off
All policy EIAs must be signed off by Mike Napier, Associate Director of Corporate Affairs
I agree with this assessment / action plan
If *disagree*, state action/s required, reasons and details of who is to carry them out with timescales:



Signed:

Date: 29.10.19