NHS
Thurrock
Clinical Commissioning Group

Information Governance

Management Framework

September 2015

Document Control:

Version:	2.2
Status:	Draft
Author / Lead:	CCGs' Information Governance Team (Hosted by Basildon & Brentwood CCG)
Board Sponsor:	Mandy Ansell, (Acting) Interim Accountable Officer and SIRO
Responsible Committee:	Audit Committee
Ratified By and Date:	
Effective From:	
Next Review Date:	
Target Audience:	NHS Thurrock CCG officers and staff (which includes temporary staff, contractors and seconded staff)

CONTENTS

APPENDICES

1 INTRODUCTION

1.1 Robust Information Governance (IG) requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. The way that an organisation chooses to deliver against these requirements is referred to within the IG Toolkit as the organisation's Information Governance Management Framework.

This framework should include detail of:

- Senior Roles
- Key Policies
- Key Governance Bodies
- Resources
- Governance Framework
- Training & Guidance
- Risk & Incident Management

2 PURPOSE / POLICY STATEMENT

2.1 The aim of this framework is to set out how the CCG will effectively manage IG. The organisation will achieve compliance by:

- Establishing robust IG processes that conform to NHS England and the Health and Social Care Information Centre (HSCIC) standards and comply with relevant legislation.
- Establishing, implementing and maintaining policies for the effective management of information.
- Providing clear advice and guidance to staff to ensure that they understand and apply the principles of IG to their working practice.
- Sustaining an IG culture through increasing awareness and promoting IG, thus minimising the risk of breaches of personal data.
- Assessing the organisation's performance using the Information Governance Toolkit and Internal Audits and developing and implementing action plans to ensure continued compliance.

2.2 Compliance with all NHS Thurrock CCG policies, procedures, protocols, guidelines, guidance and standards is a condition of employment. Breach of policy may result in disciplinary action.

3 DEFINITIONS

HSCIC	Health and Social Care Information Centre
IG	Information Governance

4 ROLES AND RESPONSIBILITIES

4.1 CCG Board

4.1.1 The CCG Board has ultimate responsibility for ensuring that the organisation corporately meets its legal responsibilities and for the adoption of internal and external governance requirements.

4.1.2 The responsibilities of the CCG Board in relation to IG are:

- To ensure IG is integrated into the broader governance of the organisation and regarded as important as financial and clinical governance in organisational culture;
- To consider outcomes from annual internal audit of IG before sign off and inclusion in the annual report;
- For the Governing Body members to undertake face to face and online IG training when it is made available;
- To review and sign off the annual IG Toolkit.

4.2 Accountable Officer

4.2.1 The Chief Operating Officer as the Accountable Officer of the CCG has overall accountability and responsibility for the management of IG and for ensuring appropriate mechanisms are in place to support service delivery and continuity in the organisation.

4.3 Senior Information Risk Owner (SIRO)

4.3.1 The role of Senior Information Risk Owner (SIRO) has been assigned to the Accountable Officer. The SIRO takes ownership of both the organisation's information risks policy and acts as advocate for information risk to the Governing Body by providing written advice on the content of the Annual Governance Statement. This includes oversight of both the organisation's information security incident reporting and response arrangements.

The key responsibilities of the SIRO are to:

- Oversee the development of an Information Risk Policy and a strategy for implementing the policy within the existing IG Framework
- Take ownership of the risk assessment process for information risk, including review of an annual information risk assessment to support and inform the Annual Governance Statement
- Review and agree actions in respect of identified information risks
- Ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff
- Provide a focal point for the resolution and/or discussion of information risk issues
- Ensure the Governing Body is adequately briefed on information risk issues

The SIRO will be supported in their role by Thurrock IG Team.

4.4 Caldicott Guardian

4.4.1 The CCG's Caldicott Guardian is the Chief Nurse. The Caldicott Guardian has particular responsibility for protecting the confidentiality of patients/service-user's information. Acting as the 'conscience' of the CCG, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of information.

4.5 Caldicott Function

4.5.1 In NHS Thurrock CCG the Caldicott Function will be undertaken by the Essex Information Governance Steering Group

The key responsibilities of the Caldicott Function are to:

- Support the Caldicott Guardian;
- Ensure the confidentiality and data protection work programme is successfully co-ordinated and implemented;
- Ensure compliance with the principles contained within the Confidentiality: NHS Code of Practice and that staff are made aware of individual responsibilities through policy, procedure and training;
- Complete the Confidentiality and Data Protection Assurance component of the IG Toolkit, contributing to the annual assessment;
- Provide routine reports to senior management on Confidentiality and Data Protection issues.

Please see Appendix E for additional guidance on the Caldicott Guardian function.

4.6 Head of Information Governance / Data Protection Officer

4.6.1 The Head of Information Governance / Data Protection Officer (DPO) is responsible for ensuring the CCG complies with all aspects of IG and the Data Protection Act. The Head of Information Governance will ensure all tasks are undertaken in order to meet the required standards.

Key tasks will include:-

- Developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, for example, the production of an overarching high level framework document supported by relevant policies and procedures.
- Ensuring that there is top level awareness and support for IG resourcing and implementation of improvements within the CCG.
- 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 and other related policies are carried out, documented and reported;

- Ensuring that the annual assessment and improvement plans are prepared for approval by the Executive Management Team in a timely manner.
- 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. For NHS organisations this will need to be in line with requirements of the Informatics Planning component of the NHS Operating Framework for 2014/15;
- 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;
- Providing a focal point for the resolution and / or discussion of IG issues.

(The Information Governance service is a hosted service provided by the NHS Basildon & Brentwood CCG Information Governance Team. The Head of Information Governance is part of this team.)

4.7 Information Governance Champion (within CCG)

4.7.1 The Information Governance Champion for the CCG is the Head of Corporate Governance. The IG Champion is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG. The key tasks, some of which will be delegated to the IG Team, include:

- Developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities
- 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 and arrangements are carried out, documented and reported
- Ensuring that the annual assessment and improvement plans are prepared for approval by the CCG Quality and Governance Committee in a timely manner.
- 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
- 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
- Providing a focal point for the resolution and/or discussion of IG issues

4.8 Information Asset Owners

4.8.1 For information risk, IAOs are directly accountable to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets.

Information Asset Owners will:

- 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, providing assurance to the SIRO.

4.9 Freedom of Information Lead

4.9.1 The Freedom of Information (FOI) Lead's main responsibilities are to:

- Ensure the CCG complies with all aspects of the Act, associated Codes of Practice and related provisions in particular for contracting and procurement, minutes of meetings and so on;
- Provide reports to the Quality and Governance Committee highlighting resource, performance and compliance issues;
- Draft and / or maintain the currency of the organisation's Access to Information Policy;
- Ensure that all staff are aware of their personal responsibilities for compliance with the Act and adhere to organisational policies and procedures;
- Ensure training and written procedures are widely disseminated and available to all staff;
- Ensure the general public has access to information about their rights under the Act;
- Establish appropriate arrangements to deal with appeals and investigations into complaints about decisions and response times;
- Liaise and work with other functions responsible for information handling activities, for example Caldicott Guardian, data protection and information security staff;
- Contribute to or liaise with external FOI networks or groups to keep updated on 'round robin requests'.

(The Freedom of Information service is a hosted service provided by the NHS Basildon & Brentwood CCG Information Governance Team. The FOI Lead is part of this team.)

4.10 Information Governance Steering Group

4.10.1 The Information Governance Steering Group (IGSG) is made up of representatives from all CCGs in Essex and other representatives as required. Terms of Reference (ToR) for this group can be found in Appendix D of this document.

4.11 Audit Committee

4.11.1 The responsibility of this Committee is to oversee the planning and delivery of IG within NHS Thurrock CCG. Their Terms of Reference in relation to IG are:

- Systems and processes are in place for ensuring that the CCG complies with requirements for information security via compliance with Level 2 of the HSCIC IG Toolkit.
- To monitor progress against the IG Action Plan and provide assurance to the CCG Governing Body on its progress.
- To review the annual IG Toolkit for sign off by the Board.

4.12 Key Contacts within the CCG

Senior Information Risk Owner	Mandy Ansell, (Acting) Interim Accountable Officer	Mandy.ansell@nhs.net
Caldicott Guardian	Jane Foster-Taylor, Chief Nurse	Jane.foster-taylor@nhs.net
CCG IG Champion	Nicola Meeks, Head of Corporate Governance	n.meeks@nhs.net

4.13 Key Contacts within the Information Governance Team

Head of Information Governance	Jane Marley	Jane.marley@nhs.net
Essex CCGs IG Lead	Tracey van Wyk	Tracey.vanwyk@nhs.net
FOI Lead	Iain Gear	Iain.gear@nhs.net
Information Governance Advisor	Debbie Smith-Shaw	Debbie.smith-shaw@nhs.net

5 POLICY DETAIL

5.1 Information Communications and Technology Work Programme

5.1.1 Technical information security issues, operational and strategic authority rests with the Information Communication Technology (ICT) Service Provider – North East London Commissioning Support Unit (NEL CSU). The ICT service provider will ensure that the following key areas are addressed:

- A documented Information Security Assurance Plan is developed and shared with the CCG.
- The requirements for assurance, scrutiny and performance monitoring in conjunction with the CCG are outlined.

- Information Risks related to information security as part of the ICT Risk register are identified and reported on.

5.2 Information Security Responsibilities

5.2.1 The ICT Service Provider will have a nominated Information Security Officer / Manager with appropriate duties and resources.

5.2.2 The Information Security Officer / Manager will occupy a key role in the delivery of IG activities and the responsible individual should be tasked with providing advice on all aspects of information security and risk management, utilising either their own expertise or external advice.

5.2.3 The quality of their assessment of information security risks, threats and advice on controls will contribute significantly to the effectiveness of the CCG information security.

5.2.4 The key responsibilities of the Information Security Officers / Manager are to:

- Draft and / or maintain the currency of the appropriate information security policies;
- Ensure security accreditation of information systems in line with the organisation's approved definitions of risk;
- Ensure compliance with the information security components of the IG toolkit, contributing to the annual IG assessment;
- Ensure all arrangements for managing information security are effective and aligned with the organisation's information security and risk policies;
- Provide reports (to include Cyber Security threats and incidents etc.) to the senior member of management (for example SIRO / IAO or equivalent) who has responsibility for IG;
- Develop and maintain an information security assurance plan to ensure the appropriate management and prioritisation of risks;
- Co-ordinate the work of other staff with information security responsibilities;
- Co-ordinate the necessary response and resolution activities following a suspected or actual security incident or breach. Keeping the information risk lead (SIRO) and information asset owners (IAOs) informed of security incidents, impacts and causes, resulting actions and learning outcomes;
- Assist in the drafting and maintenance of system level security policies;
- Assist in the development of Business Continuity Management arrangements for key information assets;
- Advise on the development of a network security policy and controls for the secure operation of ICT networks, including remote / teleworking facilities;
- Provide advice and guidance regarding the implementation of controls to mitigate against malicious or unauthorised mobile code.
- Develop and document an action plan for the delivery of all specific activities involving Information Security.

5.3 Risk Management Programme

5.3.1 In conjunction with the ICT service provider, the CCG will ensure that a methodical information security risk assessment and management process is in place to identify, implement and manage controls in place to reduce the risk to the organisation's assets. Information risk assessments will be updated annually as well as there being a process for new information assets which will be a comprehensively scoped and formally documented plan (Privacy Impact Assessment) / programme that considers the security risks to Personal Confidential Data (PCD) and critical information assets.

5.3.2 A formal information security risk assessment will be carried out on all information assets to ensure threats and vulnerabilities are mitigated. Consideration will be given to the following areas of risk analysis and risk treatment:

5.4 Risk Analysis

5.4.1 Risk analysis steps will include risk identification, risk estimation and risk evaluation. These steps will require:

- Good working knowledge of the information asset scope, structure and its valuation.
- Detailed risk assessment consideration of threats to and vulnerabilities of the asset and its components.
- Impact assessment of likely direct and indirect consequences of loss, damage or disruption to the asset.

5.5 Risk Treatment

5.5.1 Risk treatment steps will include risk reduction, risk retention, risk avoidance and risk transfer. These steps will require consideration of:

- Risk assessment results for accuracy and completeness.
- Risk treatment options and their implications.

5.5.2 Further guidance on effective management of information risk and processes for responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information system can be found in the CCG Risk Management Policy & Strategy and Guidance for the Introduction of New Processes (Privacy Impact Assessment) Policy.

5.6 Governance Framework

Staff Contracts

5.6.1 All CCG staff contracts currently contain IG related clauses within them (see Appendix B)

Non-NHS Third Party Contracts – Data Protection and Confidentiality Clauses

5.6.2 Any non-NHS third party with whom the organisation contracts should include, as a minimum, a confidentiality clause. Basildon and Brentwood CCG also requests all third party contractors to sign a declaration that they are registered with the Information Commissioners Office for data protection purposes and that they encrypt all mobile devices to minimum standard required by the NHS. (See Appendix B)

Acute Trust Contract

5.6.3 The CCG uses the standard NHS contract for Acute Trusts which includes clauses relating to IG (See Appendix B). For 2015/16 IG has also been included in Contract Monitoring (See Appendix C).

5.7 Incident Management

5.7.1 The CCG has an overarching Incident Reporting Framework which includes a section about taking into account the Social Care Information Centre (HSCIC) Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation (June 2013). The IG Team will use the criteria within the checklist document to work out the seriousness of a reported incident. The current procedure for such incidents can be found at Appendix G. Any changes to the guidance will be taken to the Information Governance Steering Group for consideration and escalation.

5.8 Openness

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

5.8.2 Information will be defined and where appropriate kept confidential, underpinning the Caldicott Principles and the regulations outlined in the Data Protection and Freedom of Information Acts.

5.8.3 Non-confidential information about the CCG and their services will be available to the public through a variety of means including the procedures established to meet requirements in the Freedom of Information Act 2000.

5.8.4 The CCG will ensure that, where it holds Personal Confidential Data (PCD) with clear legal basis to do so, the data will be shared with registered and regulated health and social care professionals who have a legitimate relationship with the individual for the purposes of direct patient contact or patient care. Further on Caldicott 2 review (to share or not to share) can be found on the HSCIC website: http://www.hscic.gov.uk/article/3638/Personal-data-access-FAQs

6 MONITORING COMPLIANCE

6.1 The CCG will use a variety of methods to monitor compliance with the processes in this document, including as a minimum the following two methods:

6.2 IG Toolkit

6.2.1 Overall compliance with this framework will be reviewed annually through review arrangements for IG required by the IG Toolkit and reported to the CCG Quality and Governance Committee and Governing Body.

6.3 IG Incidents

6.3.1 IG compliance will be monitored quarterly through the monitoring of reported IG incidents.

6.3.2 In addition to the monitoring arrangements described above, the CCG may undertake additional monitoring of this framework as a response to the identification of any gaps, or as a result of the identification of risks arising from the framework prompted by incident review, external reviews or other sources of information and advice.

6.4 Dissemination and implementation

6.4.1 This document will be published on the CCG's intranet. Managers are required to ensure that their staff understands how IG applies to their practice role/s. Awareness of any new content / change in process will be through the staff bulletin in the first instance. Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the IG Leads with the support of the Caldicott Guardian, SIRO and IG Champion.

7 STAFF TRAINING

7.1 The CCG includes IG as part of its mandatory training for all staff annually.

7.2 All new staff are required to complete the Introduction to IG training module via the online IG Training Tool, when they first join the CCG unless they have completed appropriate IG training within the last year and can evidence this.

7.3 The CCG also requires all existing staff to complete online IG training annually; if they have previously completed the Introduction to IG they can complete the Refresher Module.

7.4 The CCG has identified other modules of the IG Training Tool that those with roles relating to IG will be required to undertake (see Appendix F). Those staff members involved will be informed of the additional modules that they are required to complete, these will be completed using the IG training Tool.

7.5 In addition to the above any member of staff involved in an IG related incident may be required to undertake one or more modules of the IG Training Tool, the modules to be taken will depend on the type of incident and the outcomes of any investigations into the incident.

7.6 IG training must only be completed using the online training tool and not through the OLM system. Staff will be notified if the process for completing their training changes.

7.7 Further guidance for staff can be found in the CCGs IG related policies which can be accessed via the CCG intranet.

7.8 During 2015/16 the IG Team will be working with the appropriate CCG leads to develop an IG section on the intranet. The section will contain useful IG documentation and guidance to assist staff with their roles.

8 ARRANGEMENTS FOR REVIEW

8.1 This policy will be reviewed no less frequently than every two years. An earlier review will be carried out in the event of any relevant changes in legislation, national or local policy/guidance.

8.2 If only minor changes are required, the sponsoring Committee has authority to make these

changes without referral to the CCG Board. If more significant or substantial changes are required, the policy will need to be ratified by the relevant committee before final approval by the CCG Board.

9 ASSOCIATED DOCUMENTATION

- Information Governance Policy
- Data Protection & Confidentiality Policy
- Information Sharing Policy
- Safe Haven Policy
- Information and Cyber Security Policy
- Information Lifecycle Management Policy
- Information Risk Policy
- Essex CCGs Business Continuity Management System – Business Impact Analysis Process
- Access to Information Policy
- Acceptable Use of Electronic Communications and Portable Device Policy
- Guidance for the Introduction of New Processes (Privacy Impact Assessment) Policy
- Forensic Readiness Policy

Any new or amended policies and guidance are notified and available to staff via the CCG's Intranet. The IG Resource Guide provides additional guidance and advice to support the policies and guidance for staff. New staff members (including temporary staff, contracting staff or other CCG representatives etc.) are provided with the IG Resource Guide when they commence their employment with the CCG.

10 REFERENCES

- HSCIC Information Governance Toolkit Guidance

11 LIST OF STAKEHOLDERS CONSULTED

Date Policy Circulated	Name of Individual or Group	Were Comments Received?	Were Comments incorporated into Policy?	If no, why not?
	Mandy Ansell, (Acting) Interim Accountable Officer			
	Jane Foster-Taylor, Chief Nurse			
	Nicola Meeks, Head of Corporate Governance			

12 Results of Equality Impact Assessment

12.1 NHS Thurrock CCG recognises the diversity of the local community and those in its employment. The CCG aims to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010.

12.2 This policy is applicable to every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership.

12.3 The EIA has therefore identified no equality issues with this policy.

12.4 The EIA has been included as Appendix A.

13 Change History:

Date	Version	Author	Description
10/04/2013	0.1	NHS Central Eastern Commissioning Support Unit, Information Governance Team	New document
15/05/2013	0.2	NHS Central Eastern Commissioning Support Unit, Information Governance Team	Minor amendment following comments and recommendation from IG Steering Group.
13/06/2013	1.0	NHS Central Eastern Commissioning Support Unit, Information Governance Team	Approved by NHS Thurrock CCG Board
13/10/2014	1.1	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)	Changes in guidance and reporting structure necessitates policy review
28/11/2014	1.2	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)	Amended following comments from IG Steering Group
25/03/2015	2.0	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)	Approved by NHS Thurrock CCG Board
24/06/2015	2.1	Basildon & Brentwood CCG Information Governance Team	Document Review
14/09/2015	2.2	Head of Corporate Governance, NHS Thurrock CCG	Updating to NHS Thurrock CCG policy template

APPENDIX A

Equality Impact Assessment

To be completed and attached to any policy/procedural document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	Does the policy/guidance affect one group less or more favourably than another on the basis of:		
	▪ Race	No	
	▪ Ethnic origins (including gypsies and travellers)	No	
	▪ Nationality	No	
	▪ Gender	No	
	▪ Culture	No	
	▪ Religion or belief	No	
	▪ Sexual orientation including lesbian, gay and bisexual people	No	
	▪ Age	No	
	▪ Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2.	Is there any evidence that some groups are affected differently?	No	
3.	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	No	
4.	Is the impact of the policy/guidance likely to be negative?	No	
5.	If so can the impact be avoided?	N/A	
6.	What alternatives are there to achieving the policy/guidance without the impact?	N/A	
7.	Can we reduce the impact by taking different action?	N/A	

APPENDIX B

CONTRACT CLAUSES

STAFF CONTRACT CLAUSES

In the course of your employment you will have access to confidential information relating to your employer, its clients, patients, employees and other parties. You must not use such information for your own benefit nor disclose it to other persons without the consent of your employer and the party concerned unless required to so by law. This applies both during and after the termination of your employment. If any member of staff is found to have revealed confidential information without consent, disciplinary action may be taken which could result in summary dismissal. If you are in any doubt regarding the use of information in the pursuit of your duties, you should seek advice from your manager before communicating such information to any third party. Nothing in this clause inhibits the provisions of the Public Interest Disclosure Act 1998.

Data Protection: For the purposes of the Data Protection Act 1998 you give your consent for the Trust to hold and process personal data provided by you or relating to you for all purposes relating to your employment with the organisation. Such processing includes, but is not restricted to:

- Administration of HR and employment records, pay, employment benefits, statutory entitlements, training, employment related insurance.
- Sickness and absence records, including medical records/reports and matters relating to your fitness for work.
- Administration of the Trust's Staff Pension Scheme, e.g. calculating and paying benefits, processing 'sensitive data' such as medical details or death benefit nominations.
- Criminal records, where these are not regarded as 'spent' in accordance with the Rehabilitation of Offenders Act 1974. For posts exempt from the legislation, e.g. 'regulated positions' and posts working with children, it will also include 'unspent' convictions, cautions, reprimands and final warnings.
- The provision of references and/or information to government departments or other bodies in order to meet our obligations, e.g. Inland Revenue.
- The provision of references and/or information to other organisations when requested to do so by you, e.g. future employers, financial organisations.
- Providing information to potential purchasers of the organisation, or part of the organisation.
- The transfer of information/data within the organisation.

You shall not, during or after the termination of your employment, use improperly or disclose to others any confidential information about employees and patients of the CCG, or about the CCG's policies or finances. A breach of confidentiality during employment is regarded as gross misconduct in the CCG's Disciplinary Rules. This is available for inspection in the Human Resources Department.

CONFIDENTIALITY CLAUSES FOR NON-NHS 3RD PARTY CONTRACTS

The CONTRACTOR shall process information in accordance with the standards laid down in the Health & Social Care Information Centre (HSCIC) Information Governance (IG) Toolkit. The CONTRACTOR will have in place an IG Management Framework incorporating as a minimum a Caldicott Guardian and Data Protection Lead and have full access to adequate technical information security expertise and support. The IG Management Framework will have implemented IG related policies and procedures covering the aspects of Data Protection, Confidentiality, information sharing, information security, records management and data quality. The CONTRACTOR shall be required to have the ability to pseudonymise patient information where the COMMISSIONER requests data for service planning and performance management and any other secondary uses. IG training must be completed by all the CONTRACTOR's employees on an annual basis. The CONTRACTOR shall support the COMMISSIONER by providing relevant information to enable the COMMISSIONER to meet its obligation under the Freedom of Information Act (FOIA) 2000.

The CONTRACTOR shall, in reference to the service defined in this AGREEMENT, ensure that personal information is handled appropriately with regards to all relevant legislation. This shall include the Common Law Duty of Confidence, Data Protection Act 1998 and Article 8.1 of the Human Rights Act concerning privacy, Computer Misuse and Freedom of Information Acts.

The CONTRACTOR shall submit an annual HSCIC Information Governance (IG) Toolkit assessment and must achieve at least level 2 on all requirements or have submitted an action plan to do so, for approval by the COMMISSIONER.

Where the CONTRACTOR is processing personal data,

a. the CONTRACTOR shall have a full and current registration with the Office of the Information Commissioner.

b. the CONTRACTOR shall adhere to the Confidentiality NHS Code of Practice and Care Record Guarantee.

c. the CONTRACTOR shall be an independent Data Controller.

d. the CONTRACTOR shall inform patients about recording and use of patient information, why it is recorded and who it is disclosed to. Patients/clients shall have access to a privacy notice to support this process (formally known as a Fair Processing Notice). Verbal consent to share information with other organisations for the direct delivery of care shall be recorded in the patients' notes.

Person identifiable information (PII) shall not be shared for secondary uses (not for the direct delivery of healthcare) with other organisations, unless the CONTRACTOR has explicit patient consent, or the CONTRACTOR is required by law or if there is an overriding public interest. However, pseudonymised personal information may be shared for secondary uses.

The CONTRACTOR shall be responsible for establishing information sharing agreements with other third party organisations (including the COMMISSIONER), where the sharing of PII is necessary. The CONTRACTOR shall obtain an Information Sharing Agreement from the COMMISSIIONER for the purposes of establishing any agreements to share information.

The CONTRACTOR shall refer appropriate requests for access to health records, within 2 working days, to the COMMISSIONER's Head of Information Governance for processing.

The CONTRACTOR shall ensure that CONTRACTOR staff are provided with training about how handle PII appropriately in relation to the service provided. The CONTRACTOR shall also ensure that staff are reminded regularly of their responsibilities for safeguarding PII and that these requirements are set out in staff contracts of employment.

The CONTRACTOR shall ensure that CONTRACTOR policy and procedures regarding data protection and information security shall be readily accessible to all staff.

The CONTRACTOR shall ensure that policies, processes and procedures are established for timely, accurate and complete capture of PII related to the service, and its use. CONTRACTOR policies shall set out how checks on quality of data shall be undertaken.

The NHS number shall be used on all clinical records and correspondence in accordance with the corresponding patient safety notices.

The CONTRACTOR shall comply with the NHS Records Management Code of Practice, Schedule 2 with regards to appropriate retention and disposal requirements for the information/records collected as part of the service.

The CONTRACTOR shall dispose of all IT equipment in a secure manner, which ensures that any data held on that IT equipment is completely inaccessible, even by using specialist technical recovery techniques.

The CONTRACTOR shall ensure that all records are stored in locations which are only accessible to authorised individuals. All electronic data shall be stored on secure servers.

The CONTRACTOR shall ensure that all information systems feature appropriate access controls which allow access to the system, and the information stored therein only by authorised individuals who have a reasonable justification to access stored information.

The CONTRACTOR shall monitor the effectiveness of the controls it has in place to protect confidentiality. The CONTRACTOR shall ensure that any potential or actual breaches of practice by staff are identified, reported to the Commissioner, investigated promptly and that action is taken

to address weaknesses, in accordance with documented information security event procedures. The COMMISSIONER shall be entitled to send a representative to audit the policies and processes in place.

The CONTRACTOR shall ensure that records and systems are not at unnecessary risk from environmental hazards such as fire, theft and flood. The CONTRACTOR shall ensure that back-up copies of records are made and that such back-up copies are stored securely at an alternate safe location.

The CONTRACTOR shall ensure that records of systems are not at unnecessary risk from loss of power, corruption of data or avoidable technical failure. The CONTRACTOR shall maintain Business Continuity Plans and shall ensure that such plans are tested regularly.

The CONTRACTOR shall ensure that data is encrypted fully too current COMMISSIONER and Department of Health standards before such data is transferred electronically including by mobile devices.

Personal data shall not be transferred overseas without the express permission of the COMMISSIONER, and only under strict conditions to be determined.

The CONTRACTOR shall ensure that appropriate safeguards against loss are in place to protect PII being transported via any form of physical media. The CONTRACTOR shall adopt Safe Haven principles and procedures.

The CONTRACTOR shall forward within 2 working days of receipt any FOIA requests to the COMISSIONER'S Information Governance FOI Lead for processing.

The CONTRACTOR shall keep all records pertaining to services commissioned in accordance with section 46 of the Freedom of Information Act, to facilitate efficient retrieval of information.

The CONTRACTOR shall agree to indemnify and keep indemnified the COMMISSIONER and any beneficiary against all claims and proceedings and all liability, loss, costs and expenses incurred in connection therewith by the COMMISSIONER and any beneficiary as a result of any claim made by any individual or other legal person in respect of any loss, damage or distress caused to that individual or other legal person as a result of the CONTRACTOR's unauthorised processing or unlawful processing, destruction of and/or damage to any personal data processed by the CONTRACTOR, its employees or agents in the CONTRACTORs performance of the contract or as otherwise agreed between the parties.

ACUTE, COMMUNITY, AMBULANCE TRUST CONTRACT CLAUSES

<u>DATA PROTECTION ACT 1998 (DPA), FREEDOM OF INFORMATION ACT 2000 (FOIA) AND TRANSPARENCY</u>

The Parties acknowledge their respective duties under the DPA and FOIA and shall give all reasonable assistance to each other where appropriate or necessary to comply with such duties.

Data Protection

The PROVIDER shall achieve a minimum of level 2 assurance against all requirements in the relevant NHS information governance toolkit applicable to it. Where the PROVIDER has not achieved level 2 assurance by the Service Commencement Date, the Co-ordinating COMMISSIONER may, in its sole discretion, agree a plan with the PROVIDER to enable the PROVIDER to achieve level 2 assurance within a reasonable time.

To the extent that the PROVIDER is acting as a Data Processor on behalf of a COMMISSIONER, the PROVIDER shall, in particular, but without limitation:

- only process such Personal Data as is necessary to perform its obligations under this Agreement, and only in accordance with any instruction given by the COMMISSIONER under this Agreement;
- put in place appropriate technical and organisational measures against any unauthorised or unlawful processing of such Personal Data, and against the accidental loss or destruction of or damage to such Personal Data having regard to the specific requirements in Clause 60.4.3 below, the state of technical development and the level of harm that may be suffered by a Data Subject whose Personal Data is affected by such unauthorised or unlawful processing or by its loss, damage or destruction;
- take reasonable steps to ensure the reliability of Staff who will have access to such Personal Data, and ensure that such Staff are aware of and trained in the policies and procedures identified in Clauses 60.4.4m 60.4.5 and 60.4.6 below; and
- not cause or allow such Personal Data to be transferred outside the European Economic Area without the prior consent of the relevant COMMISSIONER.

The PROVIDER and each COMMISSIONER shall ensure that Personal Data is safeguarded at all times in accordance with the Law, which shall include without limitation obligations to:

- perform an annual information governance self-assessment using the NHS information governance toolkit;
- have an information governance lead able to communicate with the PROVIDER'S board, who will take the lead for information governance and from whom the PROVIDER'S board shall receive regular reports on information governance matters including, but not limited to, details of all incidents of data loss and breach of confidence;
- (where transferred electronically) only transfer data (i) where this is essential having regard to the purpose for which the transfer is conducted; and (ii) that is encrypted to the higher of the international data encryption standards for healthcare and the National Standards (this includes, but is not limited to, data transferred over wireless or wired networks, held on laptops, CDs, memory sticks and tapes);

- have policies which are rigorously applied that describe individual personal responsibilities for handling Personal Data;
- report all incidents of data loss and breach of confidence in accordance with the Department of Health and/or NHS England and/or the Health & Social Care Information Centre (HSCIC) guidelines;
- have a policy that allows it to perform its obligations under the NHS Care Records Guarantee;
- have agreed protocols for sharing Personal Data with other NHS organisations and (where appropriate) with non-NHS organisations; and
- where appropriate have a system in place and a policy for the recording of any telephone calls in relation to the Services, including the retention and disposal of such recordings.

Freedom of Information and Transparency

Where the PROVIDER is not a Public Authority, the PROVIDER acknowledges that the COMMISSIONERS are subject to the requirements of the FOIA and shall assist and co-operate with each COMMISSIONER to enable the COMMISSIONER to comply with its disclosure obligations under the FOIA. Accordingly the PROVIDER agrees:

- that this Agreement and any other recorded information held by the PROVIDER on the COMMISSIONERS' behalf for the purposes of this Agreement are subject to the obligations and commitments of the COMMISSIONERS under the FOIA;
- that the decision on whether any exemption to the general obligations of public access to information applies to any request for information received under the FOIA is a decision solely for the COMMISSIONER to whom the request is addressed;
- that where the PROVIDER receives a request for information under the FOIA, it will not respond to such requests (unless directed to do so by the relevant COMMISSIONER to whom the request is addressed) and will promptly (and in any event within 2 Operational Days) transfer the request to the relevant COMMISSIONER;
- that the COMMISSIONERS, acting in accordance with the codes of practice issued and revised from time to time under both section 45 of the FOIA, and regulation 16 of the Environmental Information Regulations 2004, may disclose information concerning the PROVIDER and this Agreement either without consulting with the PROVIDER, or following consultation with the PROVIDER and having taken its views into account; and
- to assist the COMMISSIONERS in responding to a request for information, by processing information or environmental information (as the same are defined in the FOIA) in accordance with a records management system that complies with all applicable records management recommendations and codes of conduct issued

under section 46 of the FOIA, and providing copies of all information requested by a COMMISSIONER within 5 Operational Days of such request and without charge.

The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of this Agreement is not Confidential Information.

Notwithstanding any other term of this Agreement, the PROVIDER hereby consents to the publication of this Agreement in its entirety including from time to time agreed changes to the Agreement subject to the redaction of information that is exempt from disclosure in accordance with the provisions of the FOIA.

In preparing a copy of this Agreement for publication pursuant to Clause 60.7 the COMMISSIONERS may consult with the PROVIDER to inform decision making regarding any redactions by the final decision in relation to the redaction of information shall be at the COMMISSIONERS' absolute discretion

The PROVIDER shall assist and cooperate with the COMMISSIONERS to enable the COMMISSIONERS to publish this Agreement

APPENDIX C

ACUTE AND COMMUNITY TRUST CONTRACT MONITORING

(1) Status of Information Governance Toolkit Assessment (i.e. started, completed, submitted) as at: 31st July, 31st October & 31st March

(2) For 31st July and 31st October: current %age score and anticipated year end %age score

(3) Prior to 31st March: current %age score split into 5 key areas (IG Management, Confidentiality & Data Protection Assurance, Information Security Assurance, Clinical Information Assurance, Secondary Use Assurance, Corporate Information Assurance)

In addition to the above the provider is to alert the CCG if at any time it does not meet the required attainment levels for the key (Statement of Compliance) criteria or will not be able to meet required timescales for submissions.

APPENDIX D

TERMS OF REFERENCE

Information Governance (IG) Steering Group

(This document is relevant to Basildon & Brentwood CCG, Castle Point & Rochford CCG, Mid Essex CCG, North East Essex CCG, Southend CCG, NHS Thurrock CCG and West Essex CCG)

1. MEMBERSHIP

Chairman	Chief Nurse NHS Basildon & Brentwood CCG
Deputy Chair	SIRO/COO North East Essex CCG
CCG Representatives	SIROs and Caldicott Guardians
Hosted IG Team Representatives	Head of IG, Essex CCGs IG Lead, FOI Lead & IG Advisor
IM&T Representative	
Other	CCG IG Champions

2. QUORACY

This group will be considered quorate when the following members, as a minimum are present:

4 CCG Representatives

2 IG Team Representatives (must include at least either Head of IG or Essex CCGs IG Lead)

3. AIMS AND OBJECTIVES

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

Organisational and managerial structures that support appropriate consideration of IG issues are essential to a properly managed IG work programme that sustains continual improvement.

To achieve this, the Information Governance Steering Group will coordinate, supervise and direct the work of others as appropriate to ensure the CCG's maintain a co-ordinated approach to IG.

This will include providing support to the SIRO and Caldicott Guardian function.

Key responsibilities of the Information Governance Steering Group

a) To inform the CCG's management and accountability arrangements for IG for the seven CCGs of Essex (North East Essex, Mid Essex, West Essex, Castle Point & Rochford, Southend, Basildon & Brentwood and Thurrock).

b) To review and update the IG strategy and associated policies.

c) To prepare the Health & Social Care Information Centre (HSCIC) Information Governance IG NHS Toolkit assessment for sign off by the CCG Boards.

d) To develop and implement the CCGs IG work programme.

e) To ensure that the CCG's approach to information handling is communicated to all staff and made available to the public

f) To provide support to staff given SIRO, Caldicott Guardian, information asset owner, data protection, confidentiality, security, information quality, records management and Freedom of Information responsibilities.

g) To monitor the CCG's information handling activities to ensure compliance with law and national guidance

h) To oversee and review significant risks on IG, information security and ensure risk management strategies are in place.

i) To oversee and review privacy impact assessments completed as a result of new/reviewed processes, services and information systems.

j) To lead on patient confidentiality and information sharing governance advice.

k) To ensure linkages are made to other assurance processes for example Care Quality Commission standards.

l) To ensure that training made available by the IG Team is taken up by staff as necessary to support them in their roles.

m) To provide a focal point for the resolution and/or discussion of IG issues.

n) To review Caldicott log incidents and issues relating to patient confidentiality and shared learning / benefits across CCGs.

4. FREQUENCY OF MEETINGS

Quarterly

5. ACCOUNTABILITY

This group will report to the:-

Quality & Governance Committee or equivalent for each CCG

6. DEPUTY ARRANGEMENTS

If neither the Caldicott or SIRO of a CCG are able to attend a substitute can be sent, however the SIRO and Caldicott will be asked to formally comment via email on any agenda item requiring approval from the CCGs.

APPENDIX E

CALDICOTT FUNCTION SPECIFICATION AND IMPLEMENTATION PLAN

In accordance with the IG Toolkit requirements the Caldicott function has been established since the inception of Primary Care Trusts. The Caldicott Guardian is required to be at Director Level and have a clinical background. The CCG's should also appoint a deputy Caldicott Guardian, also with clinical expertise, who will act on behalf of the main post holder in their absence.

The Caldicott Guardians will perform the functions as laid down in the Caldicott Guardian Manual, available on the Health & Social Care Information Centre website, and will be responsible for protecting patient and service user confidentiality and enabling information sharing. The Caldicott Guardian will also have a strategic role in representing and championing IG requirements and issues at a senior level. The role of the Caldicott Guardians will be specified and promoted throughout the IG Management Framework documentation and will be made readily accessible to staff via the CCG staff intranet. This role will be primarily supported by the NHS Code of Confidentiality.

The Caldicott Guardians will be supported by the IG team on issues concerning data protection. The FOI Lead will manage the processing of requests for access to health records and the Caldicott Guardians will provide advice on the release of information to the Police and other agencies as appropriate.

The Head of IG will negotiate and develop information sharing agreements on behalf of the Caldicott Guardians, which will be reviewed by the IG Steering Group and signed by the Caldicott Guardian.

Where CCG staff feel that meeting IG standards may cause operational difficulties or they feel that meeting IG standards would compromise patient care or safety, they can apply to the Caldicott Guardian for a decision on whether an acceptable risk status can be agreed.

Incidents and issues relating to patient confidentiality will be reported to the Caldicott Guardian promptly and recorded and monitored in the Caldicott Issues Log which will be reviewed by the IG Steering Group. The Head of Information Governance will ensure that the CCGs benefit from lessons learned by sharing at IG Steering Group meetings and, where relevant, within CCG Quality and Governance (or equivalent) Committees. The agreed acceptable risks will also be recorded in the Caldicott Issues Log.

APPENXID F

INFORMATION GOVERNANCE TRAINING TOOL MODULES

Introduction to Information Governance (or Refresher Module)	All Staff
Caldicott Guardian in the NHS & Social Care	Caldicott Guardian
NHS Information risk Management for SIRO's & IAO's	SIRO, IAOs, ISO, All IG Staff
NHS Information Risk Management (Introduction)	All IG Staff
NHS Information Risk Management (Foundation)	All IG Staff
Information Security Guidelines	Head of Information Governance and Essex CCGS IG Lead
Access to Health Records	Any staff members who have responsibility for responding to Access to Health Records requests
Records Management & the NHS Code of Practice	Any staff members who have responsibility for Records Management
Records Management in the NHS	Any staff members who have responsibility for Records Management
Patient Confidentiality	Any staff members accessing confidential or sensitive person identifiable information
Secure Transfer of Personal Data	Any staff members accessing confidential or sensitive person identifiable information

Information Governance Training (Face to Face)

Information Governance for key staff	Governing Body staff, Caldicott Guardian, SIRO, IAOs and IAAs
Information Risk Management and Information Risk Assessment	SIRO, IAOs and IAAs

APPENDIX G

NHS THURROCK CCG PROCEDURE FOR HANDLING AND REPORTING INFORMATION INCIDENTS

The Health and Social Care Information Centre (HSCIC) issued, a *Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation* (June 2013). *This guidance supersedes Checklist Guidance for Reporting, Managing and Investigating IG Serious Untoward Incidents (SUI) Gateway Ref: 13177 published in January 2010.*

The purpose for an incident investigation is to determine the facts concerning the incident and:

- To identify whether any deficiencies in the application of the CCGs policies or procedures and/or the organisation's arrangements for confidentiality and data protection contributed to the incident or;
- Determine whether a human error has occurred, but not to allocate blame;
- Establish what actually happened and what actions need to be taken to prevent reoccurrence.
- Carry out root cause analysis in order to ascertain the cause and to make recommendations

As part of an initial assessment of an incident, the IG Lead will liaise with the service area / team's IAO/s and the organisation's SIRO to ensure incidents are correctly graded and reviewed.

The IG Lead and responsible IAO/s will establish a process so that all facts are looked at and the investigation will be based on establishing what actually happened and what actions need to be taken to prevent reoccurrence, **but not to allocate blame.** However, in some cases the investigation may identify whether any disciplinary processes may need to be invoked.

The decision to notify a data subject will be made by the SIRO and the Caldicott Guardian on the grounds of disclosure, including transparency and the ability to protect against harm. This may include theft or blackmail; weighed against the potential harm that may be caused to the subject if notified of the incident.

Where an incident occurs out of business hours, the designated on-call officer will ensure that action is taken to inform the appropriate contacts within 24 hours of becoming aware of the incident.

Staff Guideline on Identifying and Reporting an Information Incident

This guideline applies to all staff including permanent, temporary and contract staff. All incidents must be reported to your line manager, Information Asset Owners (IAOs) within 24 hours of becoming aware of the incident.

What should you report?

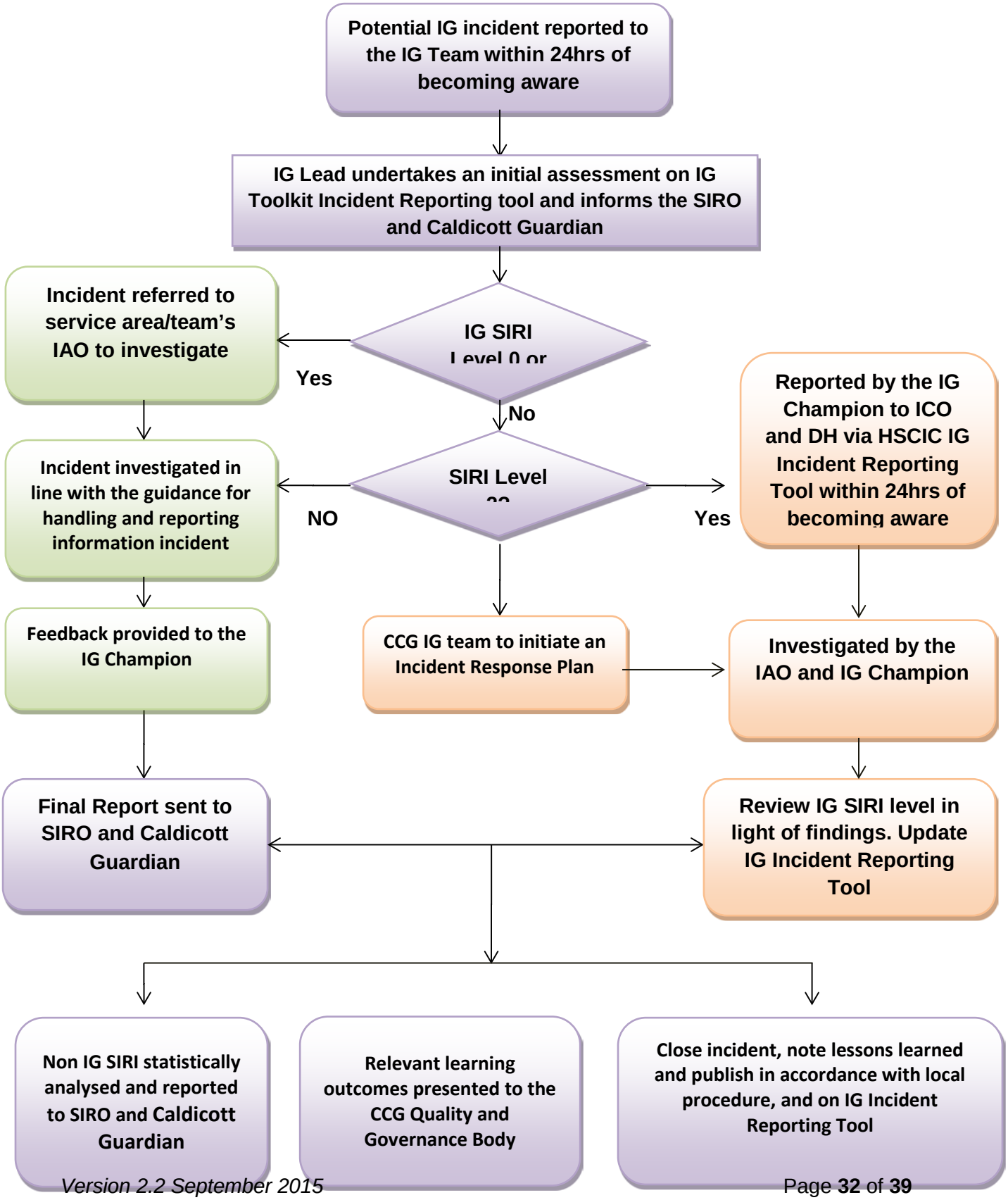
Here are some examples of information incidents that should be reported:

- Finding a computer printout of Personal Identifiable Data (PID) details laying around;
- Identifying that a fax that was thought to have been sent to a recipient had been received by an unknown recipient or organisation;
- Finding confidential waste in a 'normal' waste bin;
- Losing a mobile computing device with personal information on it;
- Giving information to someone who should not have access to it – verbally, in writing or electronically;
- Accessing a computer database using someone else's authorisation for example someone else's user id and password;
- Trying to access a secure area using someone else's swipe card or pin number when not authorised to access that area;
- Finding your PC and/or programmes aren't working correctly – potentially because you may have a virus;
- Sending a sensitive e-mail to an unintended recipient or 'all staff' by mistake;
- Finding a colleague's password written down on a 'post-it' note;
- Discovering a 'break in' to the organisation.

What happens next?

Your manager or the IG Lead member will investigate the incident and may wish to speak to you directly as things progress

Incident Management and Reporting Flowchart



Assessing the Severity of an Incident and Categorisation Process

The Health and Social Care Information Centre (HSCIC) IG Incident Reporting Tool works on the following basis when calculating the severity of an incident:

There are 2 factors which influence the severity of an IG SIRI – scale & sensitivity.

Scale Factors

Whilst any IG SIRI is a potentially a very serious matter, the number of individuals that might potentially suffer distress, harm or other detriment is clearly an important factor. The scale (noted under step 1 below) provides the base categorisation level of an incident, which will be modified by a range of sensitivity factors.

Sensitivity Factors

Sensitivity in this context may cover a wide range of different considerations and each incident may have a range of characteristics, some of which may raise the categorisation of an incident and some of which may lower it. The same incident may have characteristics that do both, potentially cancelling each other out.
For the purpose of IG SIRIs sensitivity factors may be:

i. Low – reduces the base categorisation
ii. Medium – has no effect on the base categorisation
iii. High – increases the base categorisation

Categorising Incidents

IG incident categorisation is determined by the context, scale and sensitivity. Every incident can be categorised as level:

1. Confirmed IG SIRI but no need to report to ICO, DH and other central bodies.
2. Confirmed IG SIRI that must be reported to ICO, DH and other central bodies.

A further category of IG SIRI is also possible and should be used in incident closure where it is determined that it was a near miss or the incident is found to have been mistakenly reported:

0. Near miss/non-event

Where an IG SIRI has found not to have occurred or severity is reduced due to fortunate events which were not part of pre-planned controls this should be recorded as a “near miss” to enable lessons learned activities to take place and appropriate recording of the event.

The following process should be followed to categorise an IG SIRI

Step 1: Establish the scale of the incident. If this is not known it will be necessary to estimate the maximum potential scale point

Baseline Scale	
0	Information about less than 10 individuals
1	Information about 11-50 individuals
1	Information about 51-100 individuals
2	Information about 101-300 individuals
2	Information about 301 – 500 individuals
2	Information about 501 – 1,000 individuals
3	Information about 1,001 – 5,000 individuals
3	Information about 5,001 – 10,000 individuals
3	Information about 10,001 – 100,000 individuals
3	Information about 100,001 + individuals

Step 2: Identify which sensitivity characteristics may apply and the baseline scale point will adjust accordingly.

Sensitivity Factors (SF) modify baseline scale

Low:	**For each of the following factors reduce the baseline score by 1**
-1 for each	No clinical data at risk
	Limited demographic data at risk e.g. address not included, name not included
	Security controls/difficulty to access data partially mitigates risk

Medium:	**For each of the following factors reduce the baseline score by 1**
0	Basic demographic data at risk e.g. equivalent to telephone directory
	Limited clinical information at data at risk e.g. clinical attendance, ward handover sheet

High:	**For each of the following factors increase the baseline score by 1**
	Detailed clinical information at risk e.g. case notes
	Particularly sensitive information at risk e.g. HIV, STD, Mental

+1 for each	Health, Children
	One or more previous incidents of a similar type in past 12 months
	Failure to securely encrypt mobile technology or other obvious security failing
	Celebrity involved or other newsworthy aspects or media interest
	A complaint has been made to the Information Commissioner
	Individuals affected are likely to suffer significant distress or embarrassment
	Individuals affected have been placed at risk of physical harm
	Individuals affected may suffer significant detriment e.g. financial loss
	Incident has incurred or risked incurring a clinical untoward incident

Section 3: Where adjusted scale indicates that the incident is level 2, the incident will be reported to the ICO and DH automatically via the IG Incident Reporting Tool.

Final Score	**Level of SIRI**
1 or less	Level 1 IG SIRI (Not Reportable)
2 or more	Level 2 IG SIRI (Reportable)

Example Incident Classification

Examples	
A	Health visitor data inappropriately disclosed in response to an FOI request. Data relating to 292 children, detailing their client and referral references, their ages, an indicator of their level of need, and details of each disability or impairment that led to their being in contact with the health visiting service e.g. autism, chromosomal abnormalities etc. Baseline scale factor 2 Sensitivity Factors -1 Limited demographic data 0 Limited clinical information +1 Particularly sensitive information +1 Parents likely to be distressed **Final scale point 3 so this is a level 2 reportable SIRI**

B	Imaging system supplier has been extracting PID in addition to non-identifying performance data. A range of data items including names and some clinical data and images have been transferred to the USA but are being held securely and no data has been disclosed to a third party. Baseline scale factor — 3 (estimated) Sensitivity Factors — -1 Limited demographic data 0 Limited clinical information -1 Data held securely +1 Sensitive images +1 Data sent to USA deemed newsworthy **Final scale point 3 so this is a level 2 reportable SIRI**
C	Information about a child and the circumstances of an associated child protection plan has been faxed to the wrong address. Baseline scale factor — 0 Sensitivity Factors — -1 No clinical data at risk 0 Basic demographic data +1 Sensitive information +1 Information may cause distress **Final scale point 1 so this is a level 1 SIRI and not reportable**
D	Subsequent to incident c the same error is made again and the recipient this time informs the Trust she has complained to the ICO. Baseline scale factor — 0 Sensitivity Factors — -1 No clinical data at risk 0 Basic demographic data +1 Sensitive information +1 Information may cause distress +1 Repeat incident +1 Complaint to ICO **Final scale point 3 so this is a level 2 reportable SIRI**
E	Two diaries containing information relating to the care of 240 midwifery patients were stolen from a nurse's car. Baseline scale factor — 2 Sensitivity Factors — 0 Basic demographic data 0 Limited clinical information **Final scale point 2 so this is a level 2 reportable SIRI**

F	A member of staff took a ward handover sheet home by mistake and disposed of it is a public waste bin where it was found by a member of the public. 19 individual's details were included. Baseline scale factor 1 Sensitivity Factors -1 Limited demographic data 0 Limited clinical information +1 Security failure re disposal of data **Final scale point 1 so this is a level 1 SIRI and not reportable**
G	A filing cabinet containing CDs with personal data relating to several thousand members of staff sent to landfill in error during an office move. Baseline scale factor 3 Sensitivity Factors -1 No clinical data at risk -1 Landfill unlikely to be accessed 0 Basic demographic data +1 Security failure (no encryption & poor disposal) **Final scale point 2 so this is a level 2 reportable SIRI**
H	Loss of an individual's medical records. The records were found to be missing when the patient concerned made a subject access request. Baseline scale factor 0 Sensitivity Factors 0 Basic demographic data +1 Detailed clinical information +1 Patient distressed +1 Complaint to ICO **Final scale point 3 so this is a level 2 reportable SIRI**

APPENDIX H

INFORMATION GOVERNANCE (IG) TEAM WORK PLAN (ROLLING) 2015/16

TASK	DESCRIPTION
Policy / procedure development and review	Development and ongoing review of all IG related policies and procedures.
Information Sharing Agreements (ISAs)	Supporting services in the development and monitoring of information sharing agreements with partner organisations linking with Privacy Impact Assessments and Contracts where appropriate. To maintain a register of Information Sharing Agreements. The Caldicott Guardian will oversee matters relating to confidential information, information sharing, incidents and lessons learned, ensuring legal and ethical processing of information / data supported by the information governance team.
Privacy Impact Assessments (PIAs)	Ensuring that all new systems, processes, software / hardware implementation and changes to existing are supported by Privacy Impact Assessments which are then appropriately endorsed by the SIRO and IAO.
Serious Untoward Incidents (SUIs) / Incidents	Appropriate reporting and investigation of IG / confidentiality, information security breaches, including Serious Incidents. Ensuring lessons learned are disseminated across the CCG in conjunction with existing reporting processes.
IG Toolkit	Collation of compliance evidences, implementation of requirements and monitoring of improving compliance on an ongoing basis. Working closely with CCG leads to support compliance and preparing appropriate reports for Trust Committees / Groups and submissions to Department of Health (DoH) / Health & Social Care Information Centre (HSCIC) in line with national requirements.
Training & Awareness	Development and roll-out of all training / awareness mechanisms for the CCG – to include training programmes, briefing materials (i.e. newsletter etc.), drop in sessions, poster / leaflet development (staff / patient / wider public information).

Information Asset Register / Data Flow Mapping	The SIRO and Caldicott Guardian, supported by the IG team will monitor data flows and information asset registers to identify risks. The team will ensure that identified information risks / threats are followed up, incidents managed and the appropriate Committees / Groups of the CCG are informed.
Staff/Caldicott Guardian/Senior Information Risk Owner (SIRO) Support, Advice & Guidance	Providing specialist IG support, advice and guidance to the entire CCG. Guidance and advice for all staff may be in various forms of communication (i.e. email, face to face, meetings, telephone calls, awareness articles in staff communications, reports to various meetings etc.). Providing specialist IG support to the SIRO and Caldicott Guardian to assist them with their decisions.
Project Support, Advice & Guidance	The IG Team will attend and provide specialist support, advice and guidance to ad-hoc projects within the CCG.
Meetings	The IG Steering Group will be supported by the Information Governance Team. The IG Team will attend other meetings within the CCG, as appropriate; to ensure IG is represented.
Audit (Optional – not currently part of the IG service specification)	Preparation, development and undertaking of all information governance related audits (Internal, External and local audits) – monitoring of best practice and safe systems of use of local and national applications.