INFORMATION GOVERNANCE POLICY

1. CONSULTATION AND RATIFICATION SCHEDULE	
1.2. Document Name:	Information Governance Policy
1.4. Policy Number/Version:	V4.0
1.6. Name of originator/author:	Midlands & Lancashire CSU Information Governance Team
1.8. Ratified by:	Approved at NSCCG Governing Board Approved at SOTCCG Governing Body
1.11. Name of responsible committee:	Stoke-on-Trent CCG and North Staffordshire CCG Joint Audit Committee
1.14. Date issued:	Audit Committee 15/8/17 Governing Body 5 September 2017
1.17. Review date:	September 2018
1.19. Date of first issue:	02/08/2016
1.21. Target audience:	All staff, including temporary staff and contractors, working for or on behalf of: North Staffordshire CCG and Stoke-on-Trent CCG
1.23. Purpose:	To set out the policy for Information Governance. Including the Information Governance Management Framework and Improvement Plan (Strategy for 2017/18) To detail all staff responsibilities for Information Governance and the possible consequences of not following the guidance.
1.26. Action required:	All staff are required to read and sign the declaration at the back of the Information Governance Handbook. Signing the declaration does not confirm that you are aware of everything, but confirms that you have read it and know where to refer back to in the future if required.
1.28. Cross Reference:	Information Governance Handbook
1.30. Contact Details **1.31. (for further information)**	Midlands and Lancashire CSU Information Governance Team mlcsu.ig@nhs.net / 01782 298249

33. DOCUMENT STATUS
34. This is a controlled document. Whilst this document may be printed, the electronic version posted on the CCG internet site is the controlled copy. Any printed copies of this document are not controlled. 35. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the internet.

VERSION CONTROL			
V3.1	17/07/2016	MLCSU	Minor Word Changes

Contents

1. Introduction

1.1 Information is a vital asset, both in terms of clinical management of individual patients and the efficient planning and management of services and resources.

1.2 Information Governance is a framework for handling both personal and corporate information in a confidential and secure manner. It provides a consistent way for employees to deal with the many different information handling requirements including:

- Information Governance Management
- Clinical Information assurance for Safe Patient Care
- Confidentiality and Data Protection assurance
- Corporate Information assurance
- Information Security assurance
- Secondary use assurance

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

1.4 This policy provides assurance to the CCG and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

1.5 The CCG will establish and maintain this policy and the associated procedures to ensure compliance with the requirements contained in the NHS Digital Information Governance Toolkit.

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

1.7 The role of the CCG is to commission healthcare, both directly and indirectly, so that valuable public resources secure the best possible outcomes for patients. In doing so, the CCG will seek to meet the objectives prescribed in the NHS Act 2006 and the Health & Social Care Act 2013 and to uphold the NHS Constitution. This Policy objective is to ensure that people who work for the CCG understand how to look after the information they need to do their jobs, and to protect this information on behalf of patients.

2. Aims

1.36. 2.1 The aims of this Policy are to ensure that all information created, held or processed by the CCG is:

- Held securely and confidentially
- Obtained fairly and lawfully
- Recorded accurately and reliably
- Used effectively and ethically
- Shared and disclosed appropriately and lawfully

2.2 To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental the CCG will ensure:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met
- Record inventory's will be held for all information which meets the definition of personal data
- Business continuity plans will be produced, maintained and tested
- Information Governance training will be available to all staff
- All breaches of information security, actual or suspected, will be reported and investigated.

3. Scope

1.37. 3.1 The scope of this Policy is to provide guidance to all CCG staff on the governance arrangements in relation to Information Governance.

3.2 This policy covers all aspects of information within the organisation, including but not limited to:

- Patient/client/service user information
- Employee personal Information
- Corporate information
- Business sensitive information

3.3 This policy covers all aspects of handling information, including but not limited to:

- Structured filing systems – paper and electronic
- Transmission of information – fax, email, other forms of electronic transmission such as FTP, post and telephone

3.4 This policy covers all information systems in use by the CCG and any individual directly employed or otherwise by the CCG.

3.5 The key component underpinning this policy is the annual improvement plan arising from a baseline assessment against the standards set out in the NHS Digital Information Governance Toolkit.

3.6 This policy cannot be seen in isolation as information plays a key part in corporate governance, strategic risk, service planning, performance and business management.

3.7 The policy therefore links into all these aspects of the CCG and should be read in conjunction with the respective strategies/policies.

4. Principles

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

4.2 The CCG fully supports the principles of corporate governance and recognises its public accountability. It equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff, and also corporate and commercially sensitive information.

4.3 The CCG also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

4.4 The CCG believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all CCG employees to ensure and promote the quality of information and to actively use information in decision making processes.

4.5 There are 4 key interlinked strands to the Information Governance Policy:

- Openness and Transparency;
- Legal Compliance;
- Information Security and Risk;
- Information Quality Assurance.

5. Openness & Transparency

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

5.2 Patients will have access to information relating to their own health care, options for treatment and their rights as patients. There will be clear procedures and arrangements for handling queries from patients and the public.

5.3 The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media.

5.4 Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.

5.5 Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.

5.6 The CCG will ensure that when person identifiable information is shared, the sharing complies with the law, guidance and best practice and both service users rights and the public interest are respected.

5.7 Non-confidential information relating to the CCG and its services is available to the public through a variety of media, in line with the Freedom of Information Act and Environmental Information Regulations.

5.8 The CCG will establish and maintain policies to ensure compliance with the Freedom of Information Act.

5.9 The CCG will undertake annual assessments and audits of its policies and arrangements for openness.

6. Legal Compliance

6.1 The CCG regards all identifiable information relating to patients as **confidential**. Compliance with legal and regulatory framework will be achieved, monitored and maintained.

6.2 The CCG will undertake or commission annual assessments and audits of its compliance with legal requirements through the IG Toolkit.

6.3 The CCG regards all person identifiable information relating to staff as **confidential**, except where national policy on accountability and openness requires otherwise.

6.4 The CCG will establish and maintain policies and procedures to ensure compliance with the Data Protection Act 1998 (until 24.05.18) and General Data Protection Regulations (from 25.05.18), Human Rights Act, the common law duty of confidentiality and the Freedom of Information Act and Environmental Information Regulations.

6.5 The CCG will establish and maintain procedures for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

6.6 The CCG has a comprehensive range of procedures supporting the information governance agenda; reference must be made to these alongside this policy. Legal and professional guidance should also be considered where appropriate.

7. Information Security and Risk

7.1 The CCG will establish and maintain procedures for the effective and secure management of its information assets and resources, and will ensure appropriate resilience plans are in place.

7.2 The CCG will undertake or commission annual assessments and audits of its information and IT security arrangements through the IG Toolkit framework.

7.3 The CCG will promote effective confidentiality and security practice to its staff through procedures and training.

7.4 The CCG will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security. Information Governance related incidents scoring 2 or above will be reported on the Information Governance Incident Reporting Tool to NHS England and the Information Commissioner.

7.5 The CCG will establish and maintain Risk Management and reporting procedures and will have in place risk control and monitor all reported information risks.

8. Information Quality Assurance

8.1 The CCG will establish and maintain procedures for information quality assurance and the effective management of records.

8.2 The CCG will undertake or commission annual assessments and audits of its information quality and records management arrangements in line with IG toolkit requirements.

8.3 The CCG will ensure that information is managed throughout its lifecycle of creation, retention, maintenance, use and disposal.

8.4 The CCG will ensure that information is effectively managed so that it is accurate, up to date, secure, retrievable and available when required.

8.5 Managers and employees are expected to take ownership of, and seek to improve, the quality of information within their services.

8.6 Information quality will be assured at the point of collection.

8.7 The CCG will promote information quality and effective records management through procedures and training

8.8 Wherever possible, the accuracy of information should be assured at the point of collection.

9. Training and Awareness

9.1 Information governance will be a part of an induction process.

9.2 All new and existing staff will receive annual mandatory training and guidance on information governance, which will include Caldicott and confidentiality, data protection, information security, information lifecycle management and Freedom of Information.

10. Responsibilities

10.1 It is the role of the CCG Board to define the CCG policy in respect of Information Governance, taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

10.2 The **Accountable Officer** of the CCG has overall accountability and responsibility for Information Governance in the CCG and is required to provide assurance, through the Annual Governance Statement that all risks to the CCG, including those relating to information, are effectively managed and mitigated.

10.3 The CCG Stoke-on-Trent CCG and North Staffordshire CCG Joint Audit Committee is responsible for the implementation of Information Governance Policy and Information Governance Management Framework (Strategy), and for ensuring appropriate controls and assurances are in place.

10.4 The Stoke-on-Trent CCG and North Staffordshire CCG Joint Audit Committee will monitor the performance of Information Governance, and will receive reports and other papers as necessary.

10.5 The organisation must have a **Caldicott Guardian**. This role is an amalgamation of management and clinical issues which helps to ensure the involvement of healthcare professionals in relation to achieving improved information governance compliance. The Caldicott Guardian has responsibility for ensuring that all staff comply with the Caldicott Principles and the guidance contained in the NHS Digital document – "A Guide To Confidentiality in Health and Social Care".

10.6 The Caldicott Guardian will guide the organisation on confidentiality and protection issues relating to patient information. This role is pivotal in ensuring the balance between

maintaining confidentiality standards and the delivery of patient care. The Caldicott Guardian will also advise the Board on progress and major issues as they arise.

10.7 The **Senior Information Risk Owner (SIRO)** is an Executive Director of the CCG Governing Body. The SIRO is expected to understand how the strategic business goals of the CCG will be impacted by information risks. The SIRO will act as an advocate for information risk on the Board and in internal discussions, and will provide written advice to the Accounting Officer on the content of their Annual Governance Statement in regard to information risk.

10.8 The SIRO will provide an essential role in ensuring that identified information security threats are followed up and incidents managed. They will also ensure that the Board and the Accountable Officer are kept up to date on all information risk issues. The role will be supported by the Midlands and Lancashire Commissioning Support Unit by the Information Governance Team, the CCG Caldicott Guardian, and a network of Information Asset Owners and Information Asset Administrators, although ownership of Information Risk assessment process will remain with the SIRO.

10.9 **Information Asset Owners (IAOs)** shall ensure that information risk assessments are performed at least once each quarter on all information assets where they have been assigned 'ownership', following guidance from the SIRO on assessment method, format, content and frequency. IAOs shall submit the risk assessment results and associated plans to the SIRO for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions which expected completion dates, as well as an account of residual risks.

10.10 All **managers** within the CCG are responsible for ensuring that the policy and supporting procedures are built into local processes to ensure on-going compliance. Managers are also responsible for ensuring that staff are encouraged to attend mandatory awareness training and refresher training as required.

10.11 All **staff**, whether permanent, temporary or contracted, are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

11. Monitoring/Audit

11.1 The CCG will monitor this policy and related strategies and procedures through the Stoke-on-Trent CCG and North Staffordshire CCG Joint Audit Committee.

11.2 As assessment of compliance with the requirements of the Information Governance Toolkit (IGT) will be undertaken each year. The CCG will identify staff to undertake Administrator, Reviewer and User roles as described in the IGT.

11.3 The Stoke-on-Trent CCG and North Staffordshire CCG Joint Audit Committee will ensure implementation of the Information Governance Strategy.

11.4 Annual reports and proposed action/development plans will be presented to the CCG Board for approval prior to submission of the IGT.

11.5 The policy and associated procedures will be subjected to both internal and external audit reviews.

11.6 The CCG will ensure that the support infrastructure for the SIRO is in place, and is kept under regular review.

11.7 This Policy will be made available to all Staff via the CCG website.

12. Information Governance Management

12.1 Information Governance management across the organisation will be co-ordinated by the Information Governance Group.

12.2 The responsibilities of the Stoke-on-Trent CCG and North Staffordshire CCG Joint Audit Committee will include, but not be limited to:

- Recommending policies and procedures to the appropriate CCG Board for approval.
- Recommending the annual submission of compliance with requirements in the IGT and related action plan to the CCG Board for approval.
- Co-ordinating and monitoring the Information Governance Improvement Plan (Strategy) across the organisation

12.3 The Stoke-on-Trent CCG and North Staffordshire CCG Joint Audit Committee will endorse Information Governance Improvement Plan (Strategy) for the CCG.

13. Information Governance Management Framework

13.1 The Information Governance Management Framework can be found in **Appendix A**.

14. Information Governance Improvement Plan (Strategy)

14.1 The Stoke-on-Trent CCG and North Staffordshire CCG Joint Audit Committee will be responsible for monitoring the improvement plans and associated progress.

14.2 The improvement plan is fundamental to the organisation achieving the Information Governance Toolkit. It is essential that Stoke-on-Trent CCG and North Staffordshire CCG Joint Audit Committee are updated on the progress of the plan and of any associated risks which will affect the organisations ability to achieve IG Toolkit compliance.

14.3 The Improvement Plan can be found in **Appendix B**.

15. Review

15.1 This policy and associated strategy and procedures will be reviewed on an annual basis or earlier if appropriate, to take into account any changes to legislation that may occur, and/or guidance from the Department of Health and/or NHS Executive.

16. Supporting Procedures

16.1 Information Governance Handbook.

16.2 Standard Operating Procedure for the Management of Subject Access Requests

Appendix A - Information Governance Management Framework

	Requirement	Detail
Senior Roles within the CCG	**Accountable Officer:** Marcus Warnes Accountable Officer	The Accountable Officer of the North Staffordshire CCG and Stoke-on-Trent CCG has overall accountability and responsibility for Information Governance in the CCG and is required to provide assurance through the Annual Governance Statement that all risks to the organisation, including those relating to information, are effectively managed and mitigated.
	Senior Information Risk Owner and Executive IG Lead: Alistair Mulvey Chief Finance Officer	The Senior Information Risk Owner (SIRO) is an Executive Director of the North Staffordshire CCG and Stoke-on-Trent CCG Board. The SIRO is expected to understand how the strategic business goals of the CCG may be impacted by information risks. The SIRO will act as an advocate for information risk on the Board and in internal discussions, and will provide written advice to the Accountable Officer on the content of their Annual Governance Statement in regard to information risk. The SIRO will provide an essential role in ensuring that identified information security threats are followed up and incidents managed. They will also ensure that the Board and the Accountable Officer are kept up to date on all information risk issues. The role will be supported by the Midlands and Lancashire Commissioning Support Unit Information Governance Team and the Caldicott Guardian, although ownership of the Information Risk Agenda will remain with the SIRO. The SIRO will be supported through a network of Information Asset Owners and Administrators who have been identified and trained throughout the organisation. The SIRO is also appointed to act as the overall Information Governance lead for the CCG and co-ordinate the IG work programme. The Executive IG Lead role has been assigned as Department of Health response to the Caldicott 2 Review contains an expectation that organisations across health and social care strengthen their leadership on information governance. The IG lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG, although the key tasks are likely to be delegated to an Operational IG Lead.
	Caldicott Guardian: Steve Fawcett Medical Director	The North Staffordshire CCG and Stoke-on-Trent CCG Caldicott Guardian has particular responsibility for reflecting patients' interests regarding the use of patient identifiable information and to ensure that the arrangements for the use and sharing of clinical information comply with the Caldicott principles. The Caldicott Guardian will advise on lawful and ethical processing of information and enable information sharing. They will ensure that confidentiality requirements and issues are represented at Board level and within the North Staffordshire CCG and Stoke-on-Trent CCG overall governance framework.
	Information Governance Organisational Lead: Hayley Gidman, Information Governance Lead (Midlands and Lancashire Commissioning Support Unit)	The key purpose of the role is to ensure the North Staffordshire CCG and Stoke-on-Trent CCG successfully achieves the required level of compliance across all requirements of the NHS Digital Information Governance Toolkit. The post holder will support the CCG to ensure the establishment of corporate standards and a consistent CCG wide approach to Information Governance and will be responsible for assuring the implementation of a range of policies, processes, monitoring audits and training and awareness mechanisms to ensure a high level of compliance.
	Information Governance Organisational Lead: Alex Palethorpe Head of Governance	The key purpose of the role is to ensure the North Staffordshire CCG and Stoke-on-Trent CCG successfully implements a range of policies, processes, monitoring audits and training and awareness mechanisms to ensure a high level of compliance with Information Governance & Information Security. The post holder will ensure the implementation of corporate standards and a consistent organisation wide approach to Information Governance & Information Security.

<table>
<tr><td rowspan="4">Key Policies

Policies set out the scope and intent of the organisation in relation to the management of Information Governance.</td><td>Ratification Schedule:</td><td>[IG Group]</td><td>[Audit Committee]</td><td>Board</td></tr>
<tr><td>Information Governance Policy</td><td>Insert ratification date</td><td>14/08/2017</td><td>Insert ratification date</td></tr>
<tr><td>Information Governance Hand Book</td><td>Insert ratification date</td><td>Insert ratification date</td><td>Insert ratification date</td></tr>
<tr><td colspan="4">Policies are communicated to all staff via email with the necessary documents attached. Policies are also made available on the North Staffordshire CCG Website and the Stoke-on-Trent CCG website.</td></tr>
<tr><td>Key Governance Bodies

A group, or groups, with appropriate authority should have responsibility for the IG agenda.</td><td>Audit Committee</td><td colspan="3">The North Staffordshire and Stoke-on-Trent Audit Committee is responsible for overseeing day to day Information Governance issues, developing and maintaining policies, standards, procedures and guidance, coordinating and raising awareness of Information Governance in the CCG.</td></tr>
<tr><td>Resources

Details of key staff roles</td><td>Dedicated Information Governance Staff</td><td colspan="3">Information Governance Support Officers:
Daniel Pickford - Daniel.pickford@nhs.net, 07584217105
Marie Gallagher - marie.gallagher@nhs.net, 07780228694
Gemma Hollins - g.hollins@nhs.net, 07540671326

Information Governance Manager
Name: Emma Styles
Email: emmastyles@nhs.net
Tel: 07825716409

Information Governance Lead
Name: Hayley Gidman
Email: Hayley.gidman@nhs.net
Tel: 07809320323</td></tr>
<tr><td rowspan="3">Governance Framework

Details of how responsibility and accountability for IG is cascaded through the organisation.</td><td>Information Asset Owners</td><td colspan="3">Information Asset Owners are senior individuals involved in running the relevant business.
The IAOs role is to:
- Understand and address risks to the information assets they ‘own’; and
- Provide assurance to the SIRO on the security and use of these assets.

Information Asset Owners have been nominated across the whole organisation and have received specialist information risk training to allow them to be effective in their role.</td></tr>
<tr><td>Information Asset Administrators</td><td colspan="3">The Information Asset Administrators and will:
- Ensure that policies and procedures are followed
- Recognise potential or actual security incidents
- Consult their IAO on incident management
- Ensure that information assets registers are accurate and maintained up to date.
Information Asset Owners have received specialist information risk training to allow them to be effective in their role.</td></tr>
<tr><td>Employment Contracts</td><td colspan="3">All staff and those undertaking work on behalf of the CCG need to be aware that they must meet information governance requirements and it is made clear to them that breaching these requirements, e.g. service user confidentiality, is a serious disciplinary offence.
This is supported by the inclusion of clauses within staff contracts both for substantive and temporary staff that cover Information Governance standards and responsibilities with regard to data protection, confidentiality, and information security.</td></tr>
</table>

	Contracts with Third Parties	The CCG must ensure that work conducted by others on their behalf meet all the required Information Governance standards. Where this work involves access to information about identifiable individuals it is likely that the CCG will be in breach of the law where appropriate requirements have not been specified in contracts and steps taken to ensure compliance with those requirements. Therefore the CCG endeavours to ensure that formal contractual arrangements that include compliance with information governance requirements are in place with all contractors and support organisations.
Training and Guidance Staff need clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. The approach to ensuring that all staff receive training appropriate to their roles should be detailed.	**Information Governance Handbook**	Purpose of the Handbook: • To inform staff of the need and reasons for keeping information confidential • To inform staff about what is expected of them • To protect the Organisation as an employer and as a user of confidential information This Handbook has been written to meet the requirements of: The Data Protection Act 1998 (to be superseded by the General Data Protection • Regulations on 28.05.2018) • The Human Rights Act 1998 • The Computer Misuse Act 1990 • The Copyright Designs and Patents Act 1988 • A Guide To Confidentiality in Health and Social Care (NHS Digital) This Handbook has been produced to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements. If the Handbook is breached then this may result in legal action against the individual and/or Organisation as well as investigation in accordance with the Organisation's disciplinary procedures. The Handbook will be disseminated to all staff working for the CCG and they will be required to acknowledge that they have received and understand the document. In future, any new starters to the organisation will receive a copy of this with their contract. Both should be signed and returned to their line manager and kept on file.
	Training for all staff	All staff will receive basic IG training, initially via the "Introduction to Information Governance" module of the Learning Management System *http://mlcsu.learningpool.com* 1.125. Annual refresher training will then be conducted through face to face training sessions facilitated 1.126. By the Information Governance Support Officer.
	Specialist IG training	As required specialist IG training will be provided across the organisation for those staff that are given additional responsibility for IG within their areas. Current specialist training includes: • Information Risk Training • Privacy Impact Assessments • Caldicott, Data Protection, GDPR Training
Incident Management Clear guidance on incident management procedures should be documented and staff should be aware of their existence, where to find them, and how to implement them.	**Documented Procedures and Staff Awareness**	Incident Management in the CCG is covered in the following organisational policies and Procedures: • Incident Reporting Policy • Information Governance Policy • Information Governance Handbook Staff awareness is raised through the following ways: • Staff Induction • Information Governance Training • Information Risk Training • Caldicott, Data Protection, GDPR Training

Appendix B – North Staffordshire CCG and Stoke-on-Trent CCG Information Governance Improvement Plan 2017-18

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
IG Policy Review (Required to be reviewed annually)	Review of the current policy against the newest version of the IG Toolkit, national guidance and any legislation changes within the year, including GDPR.	IG Policy	CSU IG Manager/ IG Support Officer	N/A	30th June 2017	**130 131 132 133 230**
	Review of the Information Governance Management Framework to reflect any changes in key personnel.			N/A		**231 232 235 340**
	Incorporation of the Improvement Plan for 2017-18.			N/A		**341 345 420**
Standard Information Governance Management Reporting The toolkit requires a number of standard items to be reported on a regular basis to the meeting with responsibility for Information Governance. This should be pro-active reporting (even if NIL return) rather than reactive.	Bi monthly Reporting to the organisations IG lead, Senior Information Risk Owner & Caldicott Guardian to monitor performance against the IG Improvement Plan. To include: IGT scores IG Training Information Risk Management Plan Incidents PIAs Caldicott update Data Protection requests	Bi-Monthly reports	CSU IG Manager/ IG Support Officer	N/A	Issued on or before 26th May 2017	**130 131 134**
					Issued on or before 28th July 2017	**230 231 234**
					Issued on or before 29th September 2017	**235 237 340 341**
					Issued on or before 24th November 2017	**345 346 349 350**
					Issued on or before 26th January 2018	**351 420**

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
	Information Governance Annual Report (incorporating the final Bi-monthly Report) highlighting the annual performance against the improvement plan and also sign off of the Information Governance Toolkit submission.	Annual Report		N/A	Issued on or before 16th March 2018	
<u>Information Governance Training</u> All staff are required to undertake information governance training on an annual basis ensuring that the minimum training specification set out by the Health & Social Care Information Centre is met. Additional training should be provided to staff in key roles to ensure that they remain effective within their roles and fully understand their information governance responsibilities.	All Staff Refresher Training to be delivered throughout the organisation via face to face training sessions ensuring staff are not only informed of the national responsibilities but also the organisations local implementation of legislation & guidance. This will be achieved via a 2 hour session open to all staff and will include an interactive assessment of staff training needs.	Staff Training Database detailing training completed	CSU IG Support Officer	N/A	June to December 2017	**133** **134** **230** **231** **234** **237** **340** **345** **349** **420**
	1:2:1 IG Induction sessions for new starters. All new staff to the organisation needs to be fully aware of their responsibilities in relation to information governance. To support this process a member of the Information Governance Team will meet with each new starter to take them through an IG induction which is separate to the organisation induction.	Staff Training Database detailing training completed	CSU IG Support Officer	N/A	On-going	
	Information Governance Training for Governing Body members. It is essential that all staff working on behalf of the	Staff Training Database detailing	CSU IG Manager	N/A	On request	

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
	organisation understand their responsibilities, even if they only have access to very limited information or minimal access to IT facilities. This session is optional should the CCG feel that members would benefit from high level overview training for IG.	training completed				
	Information Risk training for new staff nominated as Information Asset Owners (IAOs) or Administrators (IAAs) or where existing IAO's/IAA's require additional support. Face to face sessions to be held with the Information Governance Support Officer which will include background to information risk, roles & responsibilities and system user training.	Staff Training Database detailing training completed	CSU IG Support Officer	N/A	On-going	
	Subject Access Training for those staff identified as being responsible for the handling of Subject Access Requests under the Data Protection Act. This will be provided to staff new in the role or existing staff requiring additional support.	Staff Training Database detailing training completed	CSU IG Support Officer	N/A	On request	
	Freedom of Information training for those staff who are involved in the collation of FOI responses on behalf of the organisation.	Staff Training Database detailing training completed	CSU IG Support Officer	N/A	On request	
Information Governance Handbook	Development of an IG handbook taking into account the newest version of the IG Toolkit, national guidance, any legislation changes within the year and any lessons	IG Handbook	CSU IG Manager/ IG Support Officer CCG IG Lead to	N/A	28th July 2017	**132 133 134 230**

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
	learnt as a result of incidents within the year or areas of improvement identified via staff training, staff compliance checks and spot check audits.		support with personalisation of IG Handbook			**231 232 234 235 237 340 341 343 348 349 350 351 420**
<u>Information Governance & Data Protection Clauses within Staff Contracts</u> All staff working for or on behalf of the organisation are required to sign up to relevant clauses in relation to information governance. Clauses must be reviewed against the requirements within the toolkit to ensure that they remain up to date and fit for purpose.	Statement from most senior Human Resources Officer to confirm that all contracts of employment include adequate Information Governance clauses.	HR assurance statement	CSU IG Support Officer	N/A	30th September 2017	**132 133**
	Evidence that temporary staff and third party staff working on behalf of the organisation have signed the third party and temporary contractor agreement to ensure that they are aware that they are required to abide by the organisations information governance policies and procedures whilst undertaking work on behalf of the organisation.	List of temporary staff and third party staff working on behalf of the organisation and the date they signed the agreement	CSU IG Support Officer	N/A	Bi-Monthly check to ensure all temporary and third party staff have been identified and have signed the agreement	
<u>Contracts & Agreements Register identifying third parties with access to the organisations data</u> It is important that where a data	Through the completion of data flow mapping, it will be identified where the organisation shares data with third parties. The contracts and/or	Contracts & Agreements Register	CSU IG Support Officer	Data Flow Mapping	Bi-Monthly check to ensure all contracts	**132 344 350**

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
controller appoints a data processor on their behalf that there are appropriate clauses in place to ensure that the data is only used in line with the stipulations set out by the data controller.	agreements governing the data sharing will be reviewed to ensure that they contain adequate IG clauses and action plans put in place where amendments are required.				and agreements have been identified and reviewed	
	Further contracts will be held which provide potential access to organisational information assets which are not directly related to a data flow, e.g. photocopier suppliers or Internal Audit. These contracts will be identified and reviewed to determine whether they contain appropriate IG clauses and action plans put in place where amendments are required.		CSU IG Support Officer			
<u>Information Governance Compliance Checks</u> It is essential that the organisation regularly checks their own compliance against the policies and procedures approved for use. It is also essential that staff understand how to implement the policies and procedures in practice.	Working hour's compliance checks which will also include an assessment of staff understanding of the organisations policies and procedures including mobile working.	Feedback to SIRO and IG Lead Summary included in Bi-Monthly Report	CSU IG Support Officer	N/A	May 2017 July 2017 September 2017 November 2017 January 2018 March 2018	**133** **134** **231** **234** **237** **349**
	Out of hour's compliance check to ensure that staff follow the organisations policies and procedures in relation to	Feedback to SIRO and IG Lead	CSU IG Support Officer	N/A	April 2017 June 2017	

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
	clear screen & clear desk, the securing of confidential data and the overall security of the office areas.	Summary included in Bi-Monthly Report			August 2017 October 2017 December 2017 February 2018	
<u>Support the Internal Audit programme for Information Governance</u> NHS organisations are mandated to have an annual independent audit of their Information Governance Toolkit Compliance.	To work with the CCG to agree the internal audit scope and ensure that the evidence required, at the point of audit is available or a supporting plan is in place to achieve compliance where evidence is unavailable.	Agreed TOR for planned IGT audit	CSU IG Manager/ IG Support Officer	N/A	Quarter 4 2017/18	**N/A**
	To provide a response to the internal audit findings and where required implement the audit recommendations or put a plan in place to incorporate the findings into the wider work programme for the following year.	Audit response	CSU IG Manager/ IG Support Officer	N/A	Quarter 4 2017/18	
<u>Service Review Meetings</u> It is important for the CCG IG lead, Senior Information Risk Owner and the Caldicott Guardian to be kept informed on the progress of the IG improvement plan and have an opportunity to identify any issues	Initial Service Review meeting to look at how the team performed in the previous 12 months, lessons learnt, areas for improvement and the structural changes following the CSU management of change.	N/A	CSU IG Manager/ IG Support Officer CCG IG Lead, SIRO and Caldicott Guardian	CCG Availability	June – July 2017	**N/A**

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
with the IG management team.	6 month service review meeting to review progress against the improvement plan and ensure that he service delivery remains on track.	N/A	CSU IG Manager/ IG Support Officer CCG IG Lead, SIRO and Caldicott Guardian	CCG Availability	October – December 2017	
Data Transferred outside of the UK Identifying personal data transferred outside of the UK and whether there are appropriate agreements in place.	Completion of data flow mapping will highlight whether any data is transferred outside of the UK and therefore where further agreements and checks need to be put in place to ensure the legality and security of the data flows.	U Assure data flow mapping report	CSU IG Support Officer	Data Flow Mapping	On-going	**236** **350**
Confidentiality Audits It is essential that the organisation routinely monitors access to confidential information.	Audits of access to the following will be monitored: Smart Card Access Systems Access Shared Drive Access to Electronic Assets	Feedback to SIRO and IG Lead Summary included in Bi-Monthly Report	CSU IG Support Officer	Information Asset Register Systems and Software Register	30th June 2017 30th September 2017 31st December 2017 31st March 2018	**235** **343** **344** **348**
Caldicott To support the Caldicott Guardian in the implementation of the Caldicott Framework and to focus on the implementation of the recommendations of Caldicott 2.	Review documented internal procedure for the identification/reporting of Caldicott issues to ensure it is accurate and up to date.	Caldicott procedure Caldicott Log	CSU IG Support Officer CCG Caldicott Guardian	N/A	August 2017	**230** **231** **234**
	Provide support in the form of a 1:2:1 update to the Caldicott Guardian regarding their role and responsibilities.			N/A	August 2017	

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
Privacy Impact Assessments Privacy Impact Assessments have been mandatory within the NHS since 2008; however the completion of them is still quite ad hoc. There is a clear need to raise the awareness of Privacy Impact Assessments and embed the process.	Work with teams in the organisation that have responsibility for the commissioning, implementation and project management of new process and services to ensure that they understand the need to complete and the approval process, including providing training where requested.	Completed PIA checklists and questionnaires Summary included in Bi-Monthly Report	CSU IG Support Officer CCG Project/ Commissioning teams/IAOs	N/A	On-going	**237**
Information Sharing/Data Processing Agreements It is important to ensure that where the organisation will be party to the sharing of personal data that appropriate agreements are in place.	Ensure review process is in place to ensure that agreements are only signed off once they have been reviewed by the IG team against the Information Sharing Checklist and recommendations made and implemented where required.	Contracts & Agreements Register Caldicott Log	CSU IG Support Officer CCG Project/ Commissioning teams/IAOs	N/A	On-going	**132** **230** **231** **232**
Information Asset Registers All NHS organisations are required to record all information assets that it holds, in whatever format and record the access controls associated with them.	Review of the current information asset register and also the addition of further information to build on the previous years' work.	U Assure Reports Summary included in Bi-Monthly Report	CSU IG Support Officer CCG IAOs and IAAs	N/A	On-going	**341** **344** **345** **346** **351**
	Identification of business critical assets which need to be afforded additional protection and ensure their inclusion in Business Continuity Plans and organisational risk registers as appropriate.	U Assure Reports Summary included in Bi-Monthly Report	CSU IG Support Officer CCG IAOs	N/A	On-going	

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
	Information assets with a risk score of 12 and above need to be considered by the IAO and SIRO with consideration given as to whether these will be accepted risks or whether there are steps that can be taken to mitigate the risk.	Action plans Summary included in Bi-Monthly Report	CSU IG Support Officer CCG IAOs and SIRO	N/A	On-going	
Data Flow Mapping NHS organisations are mandated to record personal and commercially sensitive data which flows either internally within the organisation or external to the organisation.	Review of the recorded data flows and additional flows recorded once new assets have been added. These will include details of the controls in place when the assets are in transit.	U Assure Reports Summary included in Bi-Monthly Report	CSU IG Support Officer CCG IAOs and IAAs	Information Asset Register	On-going	**350**
Systems and Software Register Identification of information held within systems or software and the access controls associated.	Identification and risk assessment of systems and software used by the organisation to hold information assets to allow comprehensive system level security policies to be produced.	U Assure Reports - system level security policies Summary included in Bi-Monthly Report	CSU IG Support Officer CCG IAOs and IAAs	Information Asset Register	On-going	**235** **341** **344** **346** **347** **351**
Information Security Audits Recording the controls in place to ensure that assets remain safe and secure is not sufficient. The organisation needs to ensure that the controls afforded are being used and effective.	Information security audits will 'test' that the information recorded within the asset register is accurate and effective and that the organisation procedures are being appropriately followed.	Feedback to SIRO and IG Lead Summary included in Bi-Monthly Report	CSU IG Support Officer	Information Asset Register	30th June 2017 30th September 2017 31st December	**341** **350** **351**

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
					2017 31st March 2018	
Incident Management Supporting the organisation in the assessment, reporting and investigation of Information Governance breaches.	Working with the organisation to carry out a severity assessment based on the national requirements and where required working with the organisation to ensure that level 2 incidents are reported externally within 24 hours of becoming aware of the incident.	Incident reports/action plans Summary included in Bi-Monthly Report	CSU IG Support Officer	N/A	On-going	**133** **235** **349**
Mobile Working Arrangements It is essential that some staff have the ability to work away from the organisations bases to allow them to work effectively within their roles but this needs to be undertaken in a secure and managed way.	Ensure a record of all mobile workers is maintained which identifies the equipment held, their authorisation for mobile working and that they have received guidance on expected behaviours.	Mobile workers record including authorisation date, equipment held Staff Training Database detailing IG Handbook signature	CSU IG Support Officer	N/A	Bi-Monthly check to ensure records are accurate and up to date	**348**
Information Quality and Records Management It is essential that organisation manage all records appropriately and that they ensure standards around the creation, recording, review, retention and destruction	Development of an IG handbook which includes records management, taking into account the newest version of the IG Toolkit, national guidance, any legislation changes within the year and any lessons learnt as a result of incidents within the year or areas of improvement identified	IG Handbook	CSU IG Support Officer	IG Handbook	28th July 2017	**420**

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
of those records are implemented and up held.	via staff training, staff compliance checks and spot check audits.					
	Corporate records audit to be carried out to ensure that the procedures set out in the IG Handbook are adhered to and to identify any areas requiring more support.	Feedback to SIRO and IG Lead Summary included in Bi-Monthly Report		Information Asset Register	31st August 2017 28th February 2018	
GENERAL DATA PROTECTION REGULATION (GDPR)						
Awareness It is essential to ensure that decision makers and key people in the organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.	Customer Conference	Supporting Materials from the Day	IG Team	N/A	25th May 2017	**N/A**
	Targeted IG Training	Training Statistics	IG Training Officer/All Staff	N/A	20th June 2017 – 31st December 2017	**N/A**
	Completion of a gap analysis/information audit (team level) to identify which areas are either covered, or not required, based on the organisations processing operations. Where areas are identified as requiring further action, ensure that the work programme has the actions included.	Information Audit Report Outcome	Information Risk Officer/IAAs and IAOs	Customer Conference/Awareness of staff in key roles/CCG resource	28th July 2017	**N/A**
	Where areas of the organisation are identified as high risk in relation to current and ongoing compliance, entries	Risk Assessments to be	Information Risk Officer and Governance Leads	Information Audit Outcome Report	11th August 2017	**N/A**

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
	should be added to the organisations risk register.	completed for high risk teams.				
Understand what information the organisation holds You should document what personal data the organisation holds, where it came from and who the organisation shares it with.	The organisation needs to identify and document all data (as defined by the act as personal) sets for which they are responsible (including those processed by third parties), identify where it came from and who you share it with.	Information Asset Register via U Assure	IAAs and IAOs	Information Audit Outcome Report	24th November 2017	**N/A**
Communicating Privacy Information Review current privacy notices and put in plan in place for making any necessary changes in time for GDPR implementation.	Following the identification of all data sets, fair processing notices will need to be reviewed and changes made in line with GDPR. GDPR requires additional information to be included within the FPN including legal basis for processing the data, data retention periods and process for handling complaints.	Fair processing Notice entitled 'How we use your information'	IG Compliance Officer	Information Asset Register	31st January 2018	**N/A**
	The ICO also required that the notice should be provided in a concise, easy to understand and clear language. This will be in a challenge based on the level of information that needs to be provided. This will therefore be achieved through the use of a layered fair processing notice on the CCGs website, allowing high level information	Fair processing Notice entitled 'How we use your information'	IG Compliance Officer/Web Support	Information Asset Register	31st January 2018	**N/A**

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
	Review current fair processing notice for staff data. The fair processing notice needs to identify what staff data is collected and the purposes of the processing.	Staff Fair Processing Notice	CSU IG Compliance Officer	Data Flow Mapping	31st January 2018	**N/A**
Individuals Rights Ensure organisational procedures cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.	Service areas where personal information is processed need to have procedures in place to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format. Standard operating procedures will need to be developed within those teams processing data to ensure that individual's rights can be met – should requests be made.	Standard Operating procedure for teams that process personal data, tailored to the requirements of the processing requirement.	Information Asset Owners for teams processing PCD/IG Compliance Officer	Information Asset Register	31st January 2018	**N/A**
Subject Access Requests Update procedures and plan how the organisation will handle requests within the new timescales and provide any additional information.	The CCGs processes need to reflect the changes in the legislation in relation to subject access requests. If the request is processed by a third party then the CCG will need assurance that they have procedures in place to change how we process to meet the requirements.	Section in the handbook directing staff to the CSU for processing.	IG Compliance Officer	Information Audit Outcome Report	30th September 2017	**N/A**
Legal basis for processing personal data The organisation should identify the data sets which they process and record the legal basis for carrying it out and document it.	Individual's rights are strongly linked to an organisations basis for processing their personal data. For example, individuals will generally have a stronger right to have their data deleted where consent is the basis for processing.	Information Asset Register via U Assure and Fair Processing Notice	Information Risk Officer/IAOs and IAAs	Information Audit Outcome Report	24th November 2017	**N/A**

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
	Therefore it is essential that the organisation understands the basis by which each data set is processed.					
Consent Review how the organisation is seeking consent, obtaining and recording consent and whether any changes to the process need to be made.	Review all data that is held as a result of consent and asses the consent process and recording against the GDPR requirements which are far more detailed and explicit in what is required.	Information Audit Report Outcome	IG Compliance Officer	Information Asset Register	31st January 2018	**N/A**
	Where current consent mechanisms are identified as not meeting the GDPR requirement work will need to be undertaken with each service to address the shortcomings in the consent process.	Consent review report	IG Compliance Officer	Information Asset Register	31st January 2018	**N/A**
	Any areas where the consent process is not sufficient but will require significant resource to retrospectively achieve consent should be risk assessed and if required be included on the organisations risk register. If compliance cannot be achieved by 25th May 2018 then the risk needs to reflect the need to cease processing and the associated implications of this.	Amended and Compliant Consent forms	IG Compliance Officer	Information Asset Register	31st January 2018	**N/A**
Children If the organisation processes children's data they should think about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing	If it is identified that the organisation processes data sets relating to children then an assessment of the consent will need to be undertaken to bring it in line with GDPR as well as alerting the service to the point at which the terms of the consent will need to change i.e. child	Review of the current process for consent for children	IG Compliance Officer	Information Asset Register	31st January 2018	**N/A**

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
activity.	reaches their 13th birthday.					
	Where required processes for obtaining consent will need to be amended, documented and staff appropriately informed of the changes.	Standard Operating Procedure for the processing of children's data.	IG Compliance Officer	Information Asset Register	31st January 2018	**N/A**
Management of Data Breaches Ensure that the organisation has the right procedures in place to detect report and investigate a personal data breach.	Assessment of the data sets processed and held by the organisation to identify which ones would fall under the 'notification requirement' should a breach occur.	Information Asset Register via U Assure	Information Risk Officer	Information Asset Register	24th November 2017	**N/A**
	Incident reporting processes to be identified and updated to reflect the changes in requirements.	Incident Reporting Process (within the IG Handbook)	Information Compliance Manager	N/A	28th July 2017	**N/A**
Data Protection by Design and Data Protection Impact Assessments The organisation should seek to raise awareness of the need for Data Protection Impact Assessments and work out how and when to implement them within the organisation.	Identify the organisations project management processes and how PIA can become part of the project management process.	N/A	Information Risk Officer	N/A	28th July 2017	**N/A**
	Identify those staff that require data protection impact assessment training, book the sessions.	DPIA Training	Information Training Officer	N/A	28th July 2017	**N/A**
	Deliver DPIA training sessions	Training Records for DPIA	Information Training Officer/Nominated Staff	N/A	31st October 2017	**N/A**

Improvement/Requirement detail	Detail	Product	Lead/Resource	Inter-dependency	Completion Dates	IGT Req No.
	Work with the SIRO and Caldicott Guardian to identify their responsibilities in relation to the PIA process.	N/A	Information Training Officer	N/A	24th November 2017	**N/A**
Data Protection Officers The organisation should designate a Data Protection Officer, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.	Public authorities are required to designate a Data Protection Officer (DPO). The organisation needs to ensure that someone in the organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to so effectively.	N/A	CCG Board to nominate	N/A	31st March 2018	**N/A**
International If the organisation operates internationally, they should determine which data protection supervisory authority you come under.	Following completion of the Information Audit Report – this will highlight anywhere that the organisation is routinely transferring data outside of the UK or uses systems with servers outside of the UK.	Information Audit Report & Information Asset Register (via U Assure)	Information Risk Officer	N/A	31st March 2018	**N/A**
	Where assets are identified as being transferred or held outside of the UK to assess the security requirements against GDPR international transfers requirements	Assessment of international standards	Information Risk Officer	N/A	31st March 2018	**N/A**