Thinking Differently

NHS
Dudley
Clinical Commissioning Group

INFORMATION GOVERNANCE POLICY

UNIQUE REFERENCE NUMBER:	**AC/IG/013/V4**
DOCUMENT STATUS:	**Approved Audit & Governance Committee – 23/05/17**
DATE ISSUED:	**1 June 2017**
DATE TO BE REVIEWED:	**1 June 2020**

AMENDMENT HISTORY

VERSION	DATE	AMENDMENT HISTORY
V1	June 2013	Version approved by Audit Committee 19 June 2013
AC/IG/013/V1.1	December 2013	Addition of branding and formatting changes in line with Policy for Development of Policies
AC/IG/013/V1.2	February 2014	Addition of unique reference number prior to publication
V2	September 2014	Version approved by Audit Committee 26 September 2016
V3/IG/013/V3	Sept 2016	Review and update of Appendix A&B;IGMF and IG Work/Improvement Plan
V4/IG/013/V4	April 2017	Review and update of Appendix A&B;IGMF and IG Work/Improvement Plan

REVIEWERS

This document has been reviewed by:

NAME	DATE	TITLE/RESPONSIBILITY	VERSION
Donna Dallaway	June 2013	CSU Information Governance Manager	V1
Matthew Hartland	June 2013	Chief Finance Officer	V1
Julia Dixon	June 2013	Staff Side representative	V1
CSU-IG	June 2014	CSU - IG	V1.2
Emma Styles	June 2015	Information Governance Manager (South) CSU	V2
Paul Lewis-Grundy	June 2015	Governance Manager	V2
Sue Johnson	June 2015	Deputy Director of Finance	V2
Sarah Hirst	Sept 2016	CSU Information Governance Officer	V3
Sarah Hirst	April 2017	CSU Information Governance Manager	V4

APPROVALS

This document has been approved by:

NAME	DATE	TITLE/RESPONSIBILITY	VERSION
CCG Audit Committee	19 June 2013	Delegated authority from the Board	V1
CCG Audit Committee	26 September 2014	Delegated authority from the Board	V2
CCG Audit Committee	23 July 2015	Delegated authority from the Board	V3
CCG Audit Committee	23 May 2017	Delegated authority from the Board	V4

NB: The version of this policy posted on the intranet must be a PDF copy of the approved version.

DOCUMENT STATUS

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled.

RELATED DOCUMENTS

These documents will provide additional information

REFERENCE NUMBER	DOCUMENT TITLE	VERSION
	IG Handbook	V1

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 It is therefore 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.

1.3 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.

1.4 The CCG will establish and maintain this policy and the associated procedures to ensure compliance with the requirements contained in the Department of Health Information Governance Toolkit hosted by NHS Digital.

1.5 This policy, and its supporting procedures, is fully endorsed by the Board through the production of these documents and the approval in the relevant meeting minutes.

2. Scope

2.1 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

2.2 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

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

2.4 The key component underpinning this policy is the annual improvement plan arising from a baseline assessment against the standards set out in the Department of Health Information Governance Toolkit.

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

2.6 The policy therefore links into all these aspects of the CCG and should be reflected in these respective strategies/policies.

3. Principles

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

3.2 The CCG fully supports the principles of corporate governance and recognizes 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 commercially sensitive information.

3.3 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.

3.4 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.

3.5 There are 4 key interlinked strands to the information governance policy:

- Openness and transparency
- Legal compliance
- Information security and Risk
- Quality assurance

3.6 Openness & Transparency

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

- 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.

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

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

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

- 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.

- 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.

- Information Governance training including awareness and understanding of Caldicott principles and confidentiality, information security, records management and data protection will be mandatory for all staff. Information governance will be included in induction training for all new staff.

3.7 Legal Compliance

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

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

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

- The CCG will establish and maintain policies and procedures to ensure compliance with the Data Protection Act, Human Rights Act, the common law duty of confidentiality and the Freedom of Information Act and Environmental Information Regulations.

- 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).

- 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.

3.8 Information Security and Risk

- The CCG will establish and maintain procedures for the effective and secure management of its information assets and resources.

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

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

- 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.

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

3.9 Information Quality Assurance

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

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

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

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

- Employees are expected to take ownership of, and seek to improve, the quality of information within their services.

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

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

4. Responsibilities

4.1 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.

4.2 The Chief Officer as 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.

4.3 The Senior Information Risk Owner (SIRO) is an Executive Director of the CCG Board. 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.

4.4 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 Arden & GEM 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.

4.5 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.

4.6 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”.

4.7 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.

4.8 The Audit & Governance Committee is responsible for overseeing day to day Information Governance issues, developing and maintaining policies, standards, procedures and guidance, coordinating and raising awareness of Information Governance in the CCG.

4.9 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.

4.10 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.

5. Training/Awareness

5.1 Information governance will be a part of an induction process. 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 and Freedom of Information.

6. Monitoring/Audit

- The CCG will monitor this policy and related strategies and procedures through the Audit Committee.

- 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.

- The Audit & Governance Committee will ensure implementation of the Information Governance Strategy.

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

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

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

7. Information Governance Management

7.1 Information Governance management across the organisation will be co-ordinated by the Audit & Governance Committee.

7.2 The responsibilities of the Audit & Governance 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

The Audit & Governance Committee will endorse Information Governance Improvement Plan (Strategy) for the CCG.

8. Information Governance Improvement Plan

8.1 The Audit & Governance Committee will be responsible for monitoring the improvement plans and associated progress. The improvement plan is fundamental to the organisation achieving the Information Governance Toolkit. It is essential that the 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. The Improvement Plan can be found in **Appendix B**.

9. Review

9.1 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.

10. Supporting Procedures

- Information Governance Handbook.

IG Policy Appendix A - Information Governance Management Framework 2017-18

	Requirement	Detail
Senior Roles within the CCG	**Accountable Officer:** Paul Maubach, Chief Officer	The Chief Officer as Accountable Officer of the Dudley CCG and 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: Matthew Hartland, Chief Finance Officer	The Senior Information Risk Owner (SIRO) is an Executive Director of the Dudley 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 Arden & GEM 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 will be delegated to the allocated Organisational IG Lead/s
	Caldicott Guardian: Jonathan Darby, Clinical Lead	The Dudley 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 7 Caldicott Principles. The Caldicott Guardian will advise staff 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 Dudley CCG overall governance framework

	Information Governance Organisational Lead: Sue Johnson, Deputy Chief Finance Officer	The key purpose of the role is to ensure that Dudley CCG successfully implements a range of policies, processes, monitoring audits, 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
Commissioning Support Unit Staff	**Information Governance Organisational Lead:** Simon Clements, Information Governance Consultant (Arden & GEM CSU)	The key purpose of the CSU IG role is to ensure that Dudley CCG successfully achieve the required level of compliance across all requirements of the HSCIC/NHS Digital Information Governance Toolkit on an annual basis The CSU 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, training and awareness mechanisms to ensure a high level of compliance.
Key Policies Policies set out the scope and intent of the organisation in relation to the management of Information Governance.	**Ratification Schedule:**	**Audit Committee**
	Information Governance Policy	23rd May 2017
	Information Governance Hand Book	Reviewed document due to Committee August 2017
	Policies are communicated to all staff via the Intranet, Staff Briefings, IG Policy and the IG Handbook.	
Key Governance Bodies A group, or groups, with appropriate authority should have responsibility for the IG agenda.	**Information Governance Steering Group** – *Meeting frequency twice a year*	The purpose of the Information Governance Steering Group is to drive the information governance agenda, and to provide the Audit & Governance Committee with the assurance that effective fundamental mechanisms are in place within the CCG for the managing of all matters in connection with Information Governance Management and Information Security The work of the group will focus on ensuring compliance with these IG Toolkit requirement standards: • Information Governance management • Confidentiality and Data protection assurance • Information Security assurance • Clinical Information assurance

	Audit and Governance Committee – IG Sub Committee *Meeting frequency is monthly*	The Audit Committee is responsible for overseeing the day to day Information Governance issues, maintain and ratify policies, standards, procedures, guidance, as well as coordinating and raising awareness of Information Governance throughout the CCG
Resources Details of key staff roles	**Dedicated CSU Information Governance Staff**	Simon Clements, Information Governance Consultant, Arden & GEM CSU Simon.Clements@ardengemcsu.nhs.uk Sarah Hirst, Information Governance Manager, Arden & GEM CSU Sarah.Hirst@ardengemcsu.nhs.uk
Governance Framework Details of how responsibility and accountability for IG is cascaded through the organisation.	**Information Asset Owners**	Information Asset Owners are senior individuals involved in running the relevant business. The IAOs role is to: - Understand and address risks to the information assets they 'own' - Provide assurance to the SIRO on the security and use of these Information assets In the form of an annual Risk Assessment Review Information Asset Owners have been nominated across the whole organisation and have received specialist information risk training to allow them to be effective in their role
	Information Asset Administrators	The Information Asset Administrators will: - Ensure that policies and procedures are followed - Recognise potential or actual security incidents - Consult their IAO on incident management - Ensure that the Information Assets Registered are accurate and have a current year Risk Assessment scoring Information Asset Owners and Administrators have received specialist information risk management training to allow them to be effective in their role
	Employment Contracts	All staff and those undertaking work on behalf of the CCG need to be aware that they must meet information governance requirements and it is made clear to them that a breach of 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.
	Contracts with Third	The CCG must ensure that work conducted by others on their behalf meet all the required Information

	Parties	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 is to maintain a central Information Governance topic reference point for all staff on: • All topics under the IG scope • Information Security • Confidentiality • Staff responsibilities whilst at work • Safe and Secure handling/processing of confidential information • An aid to Protect the Organisation against the incorrect use of identifiable information The Handbook has been written to meet the requirements of: • The Data Protection Act 1998 • 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 (HSCIC/NHS Digital) The Handbook has been developed to give clear guidance to staff in the form of Policies, Processes and Procedures that fall under relevant Information Handling Laws and Codes of Practice on the processing of Personal, Personal Confidential Data, and Corporate Confidential Data. If these Policies, Processes and Procedures outlined in the Handbook are not followed then this may result in disciplinary procedures initiated on the individual. In addition the Individual and/or the Organisation can be investigated by the Information Commissioners Office, the independent body who uphold all relevant Information Handling Laws e.g. Data Protection Act 1998 **All staff need to sign the declaration in the IG Handbook that they have read and understood The Policies, Process and Procedures contained within it. This Declaration form can be found at the end of the IG Handbook and should be signed, scanned and kept in the staff Personnel file and produced on request for evidence of compliance to relevant Information Governance staff**
	Training for all staff	All staff will complete the CCG's chosen online solution Information Governance module in the first instance via 'Bluestream'. There after the online 'Bluestream' Information Governance module will be completed by staff on an annual current fiscal year basis. In addition to the online training requirements staff will attend an annual face to face IG Training session covering CCG specific IG related topics through the already established Staff Development Sessions. This session will be facilitated by the CSU Information Governance Lead for the CCG
	Specialist IG training	Specialist IG training will be provided for those staff identified with additional organisational responsibility that falls under the IG Framework. Current specialist training includes:

		• Information Asset Risk Management Training (SIRO and IAO/IAAs) • Privacy Impact Assessments • Caldicott Guardian and Data Protection 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: • Information Governance Policy • Information Governance Handbook • Staff awareness is raised through the following ways: • Staff Induction • Information Governance Training (face to face method) • Information Asset Risk Management Training • Caldicott Guardian and Data Protection Training

Appendix B Work/Improvement Plan 2017-18

Dudley CCG Version 1.0 IG Improvement Plan

Information Governance Work Plan 2017-18

	IMPROVEMENT/REQUIREMENT	DETAIL	INTERDEPENDENCY	RESOURCE	TIMEFRAMES	IG TOOLKIT REQUIREMENT(S)
Management and Accountabilities	**Management & Accountability**					
	Service Set-up Key deliverables required for the successful delivery of the service	Work Plan (this document)	IG Toolkit release Summer 2017	CCG IG Lead/s AGCSU IG Consultant AGCSU IG Manager/Lead	July 2017	N/A
		Training Plan (overview in full Excel document)	IG Toolkit release Summer 2017		July 2017	
		Communications Plan			July 2017	
		Reporting schedule (Calendar in full Excel document)	A&G Committee Administration		July 2017	
	Review of Not Relevant There is variance across the CSU's CCG customer base on the number of IGT Requiremnts claimed as Not Relevant (NR)	Internal Audit for 2016-17 did not highlight any issues with the NR's claimed. This will be continued to be monitored and if the IG Manager or evidence provider for the toolkit can evidence information to be uploaded then this will be completed and the CCG informed of the change.	3rd Party organisations e.g. Registration Authority Provider Organisation	AGCSU IG Manager/Lead AGCSU IG Consultant CCG IG Lead	To be monitored throughout year 2017-18	236, 342, 347, 352, & 421

	IG Management Framework document review This document forms the basis of IG service, support and delivery	Review the document to ensure it remains fit for purpose and defines the IG approach by the CCG	Approval of relevant CCG IG Groups	AGCSU IG Manager/Lead AGCSU IG Consultant	Start review April 2017 for 1st IGSG meeting - Complete by August 2017 for inclusion in the reviewed IG Policy	130
	Service Review/ Governance Group Meetings 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 with the IG management team.	IG Steering Group Meeting scheduled bi-annual for the year 2017-18. SIRO and CG in attendance. In addition to SIRO and CG membership of Audit and Governance Committee.	SIRO CG CCG IG Lead/s AGEM IG Team IG Steering Group A&G Committee	AGCSU IG Consultant AGCSU IG Manager/Lead CCG IG Lead CCG Administration staff (meetings) CCG SIRO CCG Caldicott Guardian	Bi-Annual IGSG starts April 2017 Monthly A&G Committee meetings	100, 200, 300, and 400 toolkit series requirements
		CCG IG Lead has 6 month service review meeting to review progress against the improvement plan and ensure that the service delivery remains on track. This takes place with A&GEM Service Delivery Director	A&G Service Delivery Director		As scheduled by CCG IG Lead and A&G CSU Service Director	

	Caldicott Function Improvement Plan To support the Caldicott Guardian in the implementation of the Caldicott Framework and to focus on the implementation of the recommendations of Caldicott 2.	Caldicott issues Log standing Item and regularly reported to the A&G Committee with CG membership.	IG Report to A&G Committee	AGCSU Team Caldicott Guardian	Standard item in IG Report to A&G Committee - CG Issues Log	All 200 series
		Caldicott Guardian support in the form of 1:2:1 training to support them in their role and understanding their CG responsibilities.		AGCSU IG Team Caldicott Guardian	ad hoc	
	Maturing Information Governance Management Reporting The toolkit requires a number of standard items to be reported on a regular basis to key meetings with responsibility for Information Governance. This should be proactive reporting (even if NIL return) rather than reactive.	Audit & Governance Committee schedule 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 ● PIA's completed ● SIRO update	CCG A&G Committee Meeting frequency	AGCSU IG Consultant AGCSU IG Manager/Lead	IG Report submitted to each scheduled A&G Committee Meeting 2017-18 March 2018	130 131 134 230 231 232 234 235 236 237 340 341 345 346 349 350 351 420

		● Caldicott update ● Data Protection requests				
		Information Governance Annual Report (incorporating the final Bimonthly Report) highlighting the annual performance against the improvement plan and also sign off of the Information Governance Toolkit submission.	N/A			

	Information Governance & Data Protection Clauses within Staff Contracts 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 staff are covered by Information Governance Clauses.			As part of the IG Toolkit evidence upload process	132 133
		Evidence that temporary staff and 3rd parties working on behalf of the organisation are required to abide by the organisations information governance policies and procedures whilst undertaking work on behalf of the organisation.			As part of the IG Toolkit evidence upload process	
	Contracts & Agreements Register identifying third parties with access to the organisations data It is important that where a data 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	Through the completion of data flow mapping the organisation is able to identify where data is shared with third parties either via data exchange or via a hosted system. Agreements can then be reviewed to ensure			As part of the IG Toolkit evidence upload process	132 341 344 350 351 352

	controller.	that appropriate Information Governance clauses are in place. Further work to do to evidence Level 3 information for Toolkit submission				
	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.	Work with the Caldicott Guardian and SIRO to ensure that a process is in place that agreements are only signed off once they have been reviewed against the Information Sharing Checklist and recommendations made where required.	IG Report to A&G Committee	AGCSU IG Consultant AGCSU IG Manager/Lead	on-going	230 231 232 250
Ap	**Risk**					

	Privacy Impact Assessments Privacy Impact Assessments have been mandatory within the NHS since 2008; however the completion of them appears to be inconsistent. There is a 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, services and systems to ensure that they understand the need to complete the documentation and complete the approval process.		AGCSU IG Team Key CCG staff	As and when required with the staff required to complete the PIA document	132 237 349 350 351
	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.	Development of an IAR Procedure in IG Handbook to be used by the IAOs/IAAs as part of fulfilling the requirements of the role in respect of the information assets they are responsible for	Risk assessment process	AGCSU IG Manager/Lead AGCSU IG Officer	Sept 2017	341 344 345 346 351
		Review of the current information held within information asset registers and also the addition of further information	Data Flow Mapping	AGCSU IG Manager/Lead AGCSU IG Officer IAOs and IAAs	Sept 2017	

		to the asset register to build on the previous years' work.				
		Identification of business critical assets which need to be afforded additional protection and need to be transferred onto the organisations risk register.			Sept 2017	
		Information assets with a risk score of 12 and above need to be considered by the IAO and consideration given as to whether these will be accepted risks or whether there are steps that can be taken to mitigate the risk.			Sept 2017	
		Identification of information held within systems or software and the access controls associated.			Sept 2017	

	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 current recorded flows linked to the information assets 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.	Information Asset register	AGCSU IG Manager/Lead IAOs and IAAs	May, June & July 2017	232 236 237 341 349 350
	Data Transferred outside of the UK Identifying personal data transferred outside of the UK and whether there are appropriate agreements in place.	Once data flow mapping has been completed that will highlight whether any data is transferred outside of the UK.		AGCSU IG Manager/Lead Nominated IAOs and IAAs	January 2017	132 236 350
	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	Staff understanding and ability to recognise IG incidents.	CCG Staff IAOs and IAAs AGCSU IG Manager/Lead	IG Report submitted to each scheduled A&G Committee Meeting 2017-18	133 235 349

		the incident.				
	IG Risk Register It is important that IG related risks and opportunities as a whole are proactively identified, managed and escalated accordingly in order to minimise harm and increase the benefits of the use of information	Initiate and maintain the collation of an IG risk register for review at relevant governance forums and by senior management	Risk Register is a Standing Item on IG Report to A&G Committee Information Asset register Data Flow Mapping Register PIA's IG Forum issues	CCG IG Lead AGCSU IG Consultant AGCSU IG Manager/Lead IAOs and IAAs	IG Report submitted to each scheduled A&G Committee Meeting 2017-18	232 236 237 341 345 346 347 348 349 350

	Business Continuity Planning	Confirming with relevant leads that the Business Continuity Plans are approved and in place, with a programme of testing/assurance for the continuation of the business of the CCG including IT Services Recovery Planning/assurances	IT Services recovery Plan	CCG IG/BC Leads Local IT Provider ISM AGCSU IG Consultant IAOs/IAAS	Nov 2017	345 346
Policy and Process	**Policy and Process**					
	IG Policy Review (Required to be reviewed annually)	Review and rationalise number of policies where applicable	IG Toolkit Version 15 due Summer 2017	IG Manager/Lead IG Officer	Aug 2017	130 131 132 133 134 230 231 232 234 235 340 341 342 343 344 345 346 420
		Review of the current policy against the newest version of the IG Toolkit, national guidance and any legislation changes within the year.				
		Review of the Information Governance Management Framework to reflect any changes in key personnel				

		and also the IG Steering Group start date of April 2017				
		Incorporation of the Improvement Plan for 2017-18 and any changes identified to this plan on the release of V15 IG Toolkit due Summer 2017 (Jun/Jul).				
	Information Governance Handbook Annual Review The handbook is to remain the same as a reference document including the policies and procedures etc.	Review of the current handbook against the newest version of the IG Toolkit, national guidance and any legislation changes within the year.	Policy Review Department of Health 2017 update on Data Guardian recommendations General Data Protection Regulations May 2018	IG Manager/Lead IG Officer	Jul/Aug 2017	132 133 134 230 231 232 234 235 237 340 341 343 348 349 350 351
		Revamp of the format of the document with the aim of providinga concise summary section with links to other content as reference.		IG Manager/Lead IG Officer		

		Inclusion of any lessons learnt as a result of incidents within the year or areas of improvement identified via staff training, staff compliance checks and spot check audits.		IG Manager/Lead IG Officer		
	Fair Processing Notice (FPN) Data Controllers are required to issue a fair processing notice to their service users identifying how they process data and who they share data with (data recipients).	Review of the current fair processing notice in place to ensure suitability for the forthcoming year and whether there are any new data uses that need to be reflected.	Data Flow Mapping	AGCSU Team CCG IG Team Caldicott Guardians CCG Communications Teams	Aug & Sept 2017	232 250 349 350
		Review of CCG website for visibility of the FPN in line with national guidance		AGCSU Team CCG IG Team Web developers	Sept 2017	
	People					

🟩	**Information Governance Training** All staff are required to undertake information governance training on an annual basis ensuring that he 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 will be required to complete online IG Training and complete the test for their IG Compliance for 2017-18. All Staff are offered Refresher Training to be delivered throughout the organisation via x3 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 three, 1 hour sessions open to all staff x2 at Brierley Hill and x1 at Tiled House site.	Bluestream online system	AGCSU IG Manager/Lead AGCSU IG Officer	3x sessions: September 2017 - BH October 2017 - TH November 2017 - BH January 2018 'Mop-up' session only if required Bluestream IG online and test in addition to face to face	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 need 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's induction.			On request if required. IG to Link with HR for comprehensive list of new starters	
		Information Governance Training for Governing Body members. It is essential that all staff working on behalf of the organisation understand their responsibilities, even if they only have access to				

🟩		very limited information or minimal access to IT facilities. This session is optional for those organisations that require members to be provided with high level overview training.				
		Information Risk training for those staff nominated as Information Asset Owners & Administrators. Face to face sessions to be held with the Information Governance Officer for the organisation which include background to information risk, roles & responsibilities and IAR Templates.	Included within the IAO/IAA training			

		Privacy Impact Assessment Training for those staff who need to be able to recognise the need for and undertake a PIA on behalf of the organisation.			As and when required with the staff required to complete th ePIA document	
	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.	Identification of those staff that have the ability to work 'remotely' and a check to ensure that those staff understand the processes to be followed when working remotely and the restrictions that are in place.	N/A	Provider IT security AGCSU IG Team	Sept 2017	348
		Review of current remote working procedures to ensure that they remain relevant and fit for purpose.	N/A	Provider IT security AGCSU IG Team	Sept 2017	
Assessment and Audit	**Assessment & Audit**					
	Support the Internal Audit programme for Information Governance NHS organisations are mandated to have an annual independent audit of their Information	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	CW Audit	AGCSU IG Manager/Lead	Jan - Mar 2018	N/A

	Governance Toolkit Compliance.	supporting plan is in place to achieve compliance where evidence is unavailable.				
		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.		AGCSU IG Manager/Lead	Jan - Mar 2018	
	Information Governance Compliance Checks (Spot Checks) 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.	Staff questionnaires based on IGT Requirements. Three cohorts will take place throughout the year: 1) Priority for staff with access to PCD 2) mid-year general staff 3) end of year general staff	Communications	CCG Staff AGCSU IG Manager/Lead	Aug 2017 Oct 2017 Jan 2018	133 134 231 234 237 349

		Working hours compliance checks which will also include an assessment of staff understanding of the organisations policies and procedures.		CCG Staff AGCSU IG Manager/Lead	Aug 2017 Oct 2017 Jan 2018	
		Out of hours compliance check to ensure that staff follow the organisations policies and procedures in relation to clear screen & clear desk, the securing of confidential data and the overall security of the office areas.		CCG Staff AGCSU IG Manager/Lead	2 per year depending on building access	
	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	Information Asset Register Caldicott Guardian plan and log IT & Registration Authority Provider	IAOs and IAAs AGCSU IG Manager/Lead IT & Registration Authority Provider	Combined with Spot Checks Aug 2017 Oct 2017 Jan 2018	235 343 344 348

🟨	**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 and data flows is accurate and effective and that the organisation procedures are being appropriately followed.	Information Asset Register Caldicott Guardian plan and log IT & Registration Authority Provider	IAOs and IAAs AGCSU IG Manager/Lead IT Provider	Combined with Spot Checks Aug 2017 Oct 2017 Jan 2018	341 350 351

End of Document