

**Information
Governance
Operating Model
2016 / 2017**



NHS England Information Governance Operating Model – 2016 / 2017

Version number: 0.22

First published:

Prepared by: Carol Mitchell, Head of Corporate Information Governance,
Dawn Monaghan, Head of Data Sharing & Privacy Unit

Classification: OFFICIAL

The National Health Service Commissioning Board was established on 1 October 2012 as an executive non-departmental public body. Since 1 April 2013, the National Health Service Commissioning Board has used the name NHS England for operational purposes.

OFFICIAL

1	Executive Summary.....	4
2	Introduction.....	5
	2.1 Background.....	5
	2.2 Purpose.....	6
	2.3 Scope.....	7
	2.4 Accountability and Commissioning Responsibilities.....	7
3	IG Framework – Resources and Roles.....	8
	3.1 Corporate IG Team Resources	8
	3.2 Data Sharing & Privacy Unit (DSPU) Resources.....	9
	3.3 Senior Information Risk Owner (SIRO).....	11
	3.4 Caldicott Guardians	13
	3.5 IG Groups.....	14
4	Key Stakeholders	15
5	IG Activity Areas.....	18
	5.2.1 Ad- hoc IG Support	19
	5.2.2 Strategic Programmes Support.....	21
	5.2.3 IG Support for Directly Commissioned Services – Primary Care	22
	5.2.4 Proactive Involvement in Strategic National Issues	23
	5.2.5 IG Commitments Programme	23
	5.2.6 System Wide IG Policy and Guidance	24
	5.2.7 Directions and Standards.....	24
	5.2.8 Records Management.....	24
	5.2.9 Internal IG Assurance and Legal Compliance.....	26
	5.2.10 IG Assurance for Directly Commissioned Services	27
	5.2.11 Oversight/Assurance of CCGs	29
	5.2.12 Oversight/Assurance of CSUs	30
	5.2.13 Primary Care Support England	35
	5.2.14 Data Services for Commissioners.....	36
6	IG Operating Model Glossary	38
	Appendix A: Strategic Projects and National Information Board (NIB) Domains	40
	Appendix B: Corporate IG Resources	42
	Appendix C: DSPU Team Structure	45
	Appendix D: SIRO Responsibility and Assurance for NHS England, CCGs and CSUs	46
	Appendix E: Terms of Reference.....	52
	Appendix F: Internal IG Assurance and Legal Compliance	53
	Appendix G: Corporate IG Team Objectives 2016-17	65

1 Executive Summary

1.1 Purpose

This operating model sets out the operating arrangements for the provision of a high quality and effective Information Governance (IG) service across NHS England. It is intended to:

- Provide clarity regarding the roles and responsibilities of both the Corporate IG team and the Data Sharing and Privacy Unit
- Describe the roles and responsibilities for Corporate IG within the central team, regional and locality teams
- Define the roles and responsibilities for deputy Senior Information Risk Owners and local Caldicott Guardians

The document describes:

- The overarching IG framework
- The IG resources and roles within NHS England
- The activities of the two IG teams and how the IG service is delivered
- The key stakeholders for the IG activities
- The assurance processes for NHS England's commissioning activities

The operating model can be used by both NHS England staff and external bodies to locate where, when and how to seek IG advice. It provides details of escalation and approval processes and raises awareness of the need to seek IG advice, where appropriate, at the start of programmes/projects e.g. by undertaking privacy impact assessments.

The document provides a useful reference tool as various policies and procedures are embedded within the document.

1.2 IG Activity Areas

The work of the DSPU and Corporate IG team has been divided into 14 activity areas and this document defines the responsibility for each area and describes how each activity is undertaken.

The two IG teams are working together to make the best use of resources and to make it easier for people to know where to direct enquiries. There is one mailbox where all emails are received and a joint business support function will triage them to the relevant team for action.

Staff located in regional/ local teams should contact their region IG lead/ local team IG officer as appropriate for local support or guidance.

The team are also looking at other ways of joint working e.g. a joint newsletter and intranet site.

1.3 IG Assurance

OFFICIAL

NHS England must satisfy itself (a) that we treat data securely and lawfully ourselves and (b) that all NHS organisations from which we commission services, either directly or indirectly through Clinical Commissioning Groups (CCGs) in England are doing likewise.

There were gaps in NHS England's ability to assure (i) Commissioning Support Units' (CSUs) cyber and IG assurance, and (ii) in assuring CCGs' IG arrangements including how they discharge their responsibility for assuring their services they commission.

Proposals were made to strengthen the assurance arrangements and mitigate risk by extending NHS England's Senior Information Risk Owner's (SIRO) responsibilities to include accountability for;

- Cyber security across NHS England's specific areas of responsibility and accountability
- CSUs IG and cyber security assurance
- CCGs IG arrangements;
- CCGs are providing assurance regarding their commissioned service providers

This operating model describes the assurance processes that seek to address the above.

2 Introduction

2.1 Background

When NHS England was established in 2013 two teams with Information Governance (IG) responsibilities were formed:

- **The Corporate IG team**, within the Transformation and Corporate Operations directorate (TCO), are responsible for internal IG arrangements and records management. These include policies and procedures, information sharing agreements, management of security incidents, IG training, IG toolkit, information security and data protection compliance, support to the Caldicott Guardian and Senior Information Risk Owner (SIRO).

The Corporate IG team currently consists of 7 members of staff in the central team and 4 regional IG leads who are supported by locality IG officers. The funding for the regional IG leads was transferred from TCO to Commissioning Operations when funding was provided for the locality IG officers.

- **The Strategic IG team (now known as Data Sharing & Privacy Unit)**, within the Operations and Information directorate are responsible for outward facing strategic IG, working with key external stakeholders such as the Department of Health, NHS Digital, Care Quality Commission, Public Health England, Information Commissioner's Office etc. They ensure we meet our statutory functions in relation to IG, such as drafting directions and contributing to information standards, proactively assisting programmes with IG considerations,

OFFICIAL

strategies and implementation and providing advice and guidance to the NHS as a whole.

The team presently has six members of admin funded staff, supplemented by programme staff on fixed term contracts as and when appropriate.

Following the re-structuring under the Organisational Alignment and Capabilities Programme (OACP), the two teams have worked together to undertake a review to clarify the respective roles and responsibilities of the Corporate IG and the Data Sharing and Privacy Unit (DSPU) In particular, a review has been undertaken to identify responsibilities that were orphaned as a result of OACP.

In addition to the two IG teams, an IG framework has been established consisting of:

- National IG Steering Group
- Central Team IG Operational Group
- Region IG Operational Groups
- Deputy SIROs appointed in regions to support the National SIRO
- Local Caldicott Guardians appointed in the region and their local teams to support the National Caldicott Guardian.

The roles and responsibilities for the above resources were not clearly defined and this operating model seeks to make it clear where responsibility lies for the various tasks and escalation process.

In addition, there was often confusion with regard to the responsibilities for hosted bodies e.g. CSUs and the operating model will seek to clarify their roles and responsibilities.

2.2 Purpose

The purpose of this document is to set out the operating arrangements for the delivery of IG across NHS England. It is intended to:

- Provide clarity regarding the roles and responsibilities of both the Corporate IG team and the Data Sharing and Privacy Unit
- Describe the roles and responsibilities of Corporate IG within the central team, regions and local teams and hosted bodies
- Define the roles and responsibilities of deputy SIROs and local Caldicott Guardians

The document describes:

- The overarching IG framework
- Details the IG resources and roles within NHS England
- Describes the activities of the combined IG teams and how the IG service is delivered
- Identifies the key stakeholders for the IG activities

2.3 Scope

This operating model describes the IG activities of NHS England which have been divided into 14 activity areas, as shown in the diagram in Section 5.1 and further described in detail in Section 5.2.

Strategic projects that have been identified for the next 1-3 years are shown in Appendix A.

2.4 Accountability and Commissioning Responsibilities

Whilst NHS England's main functions are in relation to commissioning, both as a direct commissioner of primary and specialised care and indirectly through the CCGs, NHS England also has wider statutory functions in relation to the health and care system. NHS England provides guidance to both providers and commissioners on IG, to identify, create and use levers that ensure minimum standards of IG are met and also to create an environment of continuous improving practice. This provides better safeguards for patients and also keeps pace with the rapidly evolving environment.

NHS England's statutory obligations have been documented separately in *NHS England Information Governance: Relevant functions, duties and powers*. NHS England's key legal responsibilities are set out below:

- a) First, NHS England must itself comply with the legal framework governing the use of information in the exercise of its powers¹. This includes both ensuring its own internal compliance with legal requirements but also ensuring it only commissions services from providers that are legally compliant. In the context of the use of patient information this includes a positive obligation on NHS England as a public body to protect and promote the privacy of individuals under the Human Rights Act 1998². As many of the functions previously performed by Primary Care Trusts (PCTs) have transferred to NHS England³ such as the commissioning of primary and specialised care services, NHS England therefore also has responsibility for holding such providers to account for the services provided including the effective and lawful use of personal and confidential information;
- b) NHS England's duties to exercise its functions efficiently and effectively⁴ and with a view to securing continuous improvement in the quality of services⁵ also apply to IG. Good IG not only ensures legal compliance but facilitates high quality and efficient care through the lawful and ethical use of patient information. Identifying, creating and using levers to improve IG therefore supports effective care and efficient services.
- c) NHS England must publish guidance on the processing of information to providers registered with the CQC, across both health and social care⁶;

¹ Overarching legal framework but illustrated by contract provisions.

² Article 8 of the European Convention on Human Rights as enacted by the Human Rights Act 1998

³ For example responsibilities related to GP and other primary care commissioning under the GMS and PMS Contract regulations and commencement and transitional orders related to the H & SC Act 2012

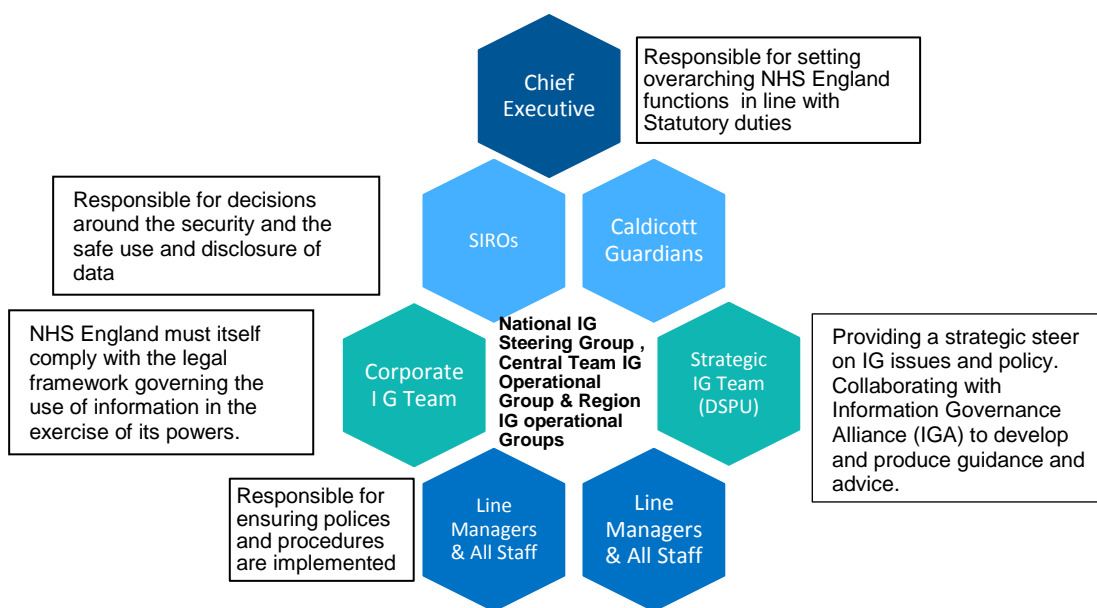
⁴ Section 23 of the H & SC Act 2012 which created a new section 13D in the NHS Act 2006

⁵ Section 23 of the H & SC Act 2012 which created a new section 13E in the NHS Act 2006

⁶ Section 23 of the H & SC Act 2012 which created a new section 13S in the NHS Act 2006

- d) NHS England must publish guidance on commissioning for CCGs for which IG is a key component⁷;
- e) NHS England alongside the Secretary of State has responsibility for Information standards, which include those related to IG⁸;
- f) The Mandate from the Government sets out the list of requirements for NHS England to fulfil each year. Many of these activities involve the use of patient data and therefore IG is essential to ensure the lawful and effective use of such information to achieve these purposes⁹;
- g) NHS England is also under an obligation to promote the NHS Constitution¹⁰ which includes key requirements in relation to the use of patient information;
- h) NHS England is empowered to issue directions to NHS Digital¹¹ and others to enable the lawful flow of data where permitted through its statutory functions.

3 IG Framework – Resources and Roles



3.1 Corporate IG Team Resources

The Corporate IG team currently consists of 7 staff in the central team (Transformation and Corporate Operations directorate) who are supplemented by 4 regional IG leads (Commissioning Operations directorate). The regional IG leads are supported by locality IG

⁷ Section 26 of the H & SC Act 2012 which created a new section 14Z8 in the NHS Act 2006

⁸ Sections 250 & 251 of the H & SC Act 2012

⁹ Section 23 of the H & SC Act 2012 which created a new section 13A in the NHS Act 2006

¹⁰ Section 23 of the H & SC Act 2012 which created a new section 13C in the NHS Act 2006

¹¹ Under Section 254 of the H & SC Act 2012

OFFICIAL

officers. Each local team has also nominated a senior IG lead and a summary of these roles and the region IG lead role is provided in Appendix B together with the current structure charts for the Corporate IG team and the regional teams.

Dedicated IG staffing resources (permanent):

Central Team	Regional teams	Localities
Head of Corporate IG	Regional IG Lead x 4	IG Officers x 12
Deputy Head of Corporate IG/ Data Assurance Lead		
IG Lead - Central		
IG Officer - Central		
Records Manager		
Records Management Officer		
Commissioning Graduate - IG		
Business Support		

Additional IG supporting roles:

Central Team	Regional Teams	Local offices
National SIRO	Deputy SIRO x 4	Nominated IG lead x 12
Deputy SIRO	Local Caldicott Guardians x 4	Local Caldicott Guardians x 12
National Caldicott Guardian		
Deputy Caldicott Guardian		

The Corporate IG team are responsible for providing an IG service across NHS England and in order to do this effectively and efficiently all the IG resources need to work together. NHS England is undertaking a single IG Toolkit assessment and this requires a significant amount of cooperation and co-ordinated working between the central IG team and the region IG leads and their local team IG officers. This operating model seeks to clearly define the roles and responsibilities needed to ensure that the IG Toolkit assessment is undertaken efficiently and with the desired outcome.

The operating model identifies the responsibilities for other significant tasks that are undertaken e.g. incident reporting and management, subject access requests, ICO investigations, information asset management, risks and issues etc.

3.2 Data Sharing & Privacy Unit (DSPU) Resources

The DSPU consists of 6 permanent staff formed of 1 Head of Unit, 1 programme/project manager 3 IG 'specialists' and 1 admin support. Additionally the unit also has temporary staff who support the programme and project work undertaken by the unit. These additions equate to an additional 7 temporary posts. The team head count should be 13, however it is presently 7, the team has been recently profiled and recruitment is underway. A business case has also been approved to provide contingency should an increase in workload be created through work streams emanating from the National Information Board (NIB) Domains. Programmes will occasionally fund IG staff directly from their programme budgets and it is hoped that in the future these staff will be recruited and line managed by DSPU with a dotted line to the programme management.

OFFICIAL

On a day to day basis the DSPU are responsible for proactively identifying and understanding what is happening within the Health and Social care sector and ensuring that strategy is developed and implemented to meet the needs of our external stakeholders. This includes facilitating support for strategic programmes and projects across NHS England. DSPU works closely with programme managers, scoping the programme/project fully in order to ensure IG needs are identified early in the process, finding solutions and implementing guidance where required.

DSPU ensure that NHS England's IG statutory duties are met in several ways:

- Collaborating with the IGA to identify, prioritise, commission, develop, draft, endorse and publish national guidance
- Drafting directions
- Assist in the development and drafting of standards and frameworks
- Liaise with other key external stakeholders such as DH and the National data Guardian
- Approving gateway reviews for IG
- Assisting with Section 251 applications where appropriate
- Answering IG enquiries
- Attending and contributing to national level events
- Hosting national events when appropriate.

DSPU Resources:

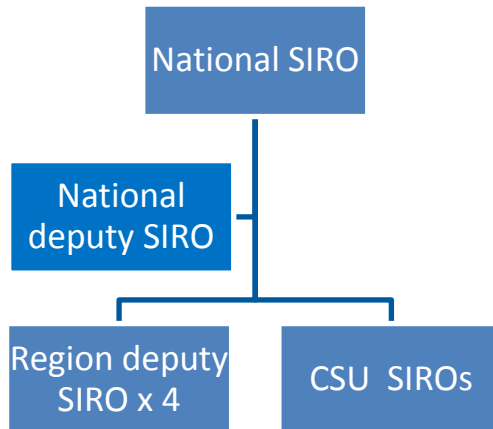
DSPU	Permanent	Non-permanent staff
Head of DSP	1.0 wte	
Senior IG Specialist	1.0 wte	
Senior IG General Manager	1.0 wte	
2 IG Specialists	1.0 wte	
Admin Support	1.0 wte	
IG Specialist		1.0 wte
IG Lead (IGA)		0.4 wte

Programme vacancies within recruitment process

Currently within recruitment process for;	Non-permanent staff
3 x IG Leads (Projects)	1.0 wte
2 x IG Support (Projects)	1.0 wte

3.3 Senior Information Risk Owner (SIRO)

3.3.1 NHS England's SIRO framework



The National Director of Transformation and Corporate Operations has been appointed as NHS England's National SIRO. As NHS England is a very large organisation, deputy SIROs have been appointed in the central team, each regional team and CSUs, to provide support to the national SIRO. They are accountable to the National Director Transformation and Corporate Operations as SIRO for NHS England as a whole.

3.3.2 National SIRO

Alongside the general roles and responsibilities of a SIRO, NHS England's national SIRO also has additional responsibilities in relation to the wider NHS and care system.

These wider system responsibilities align with NHS England's statutory responsibilities which include ensuring NHS England provides guidance to providers registered with the CQC in relation to the processing of information, and ensuring that commissioners both hold providers to account for the effective management of their information assets and risks and conform with requirements themselves¹².

The national SIRO also has a strategic role in championing effective information risk management across the service, working with DSPU in liaising with key stakeholders such as the Department of Health and NHS Digital, both individually, and as part of the Information Governance Alliance. The purpose of this liaison work is to collaborate on system wide issues and solutions. The national SIRO also shares responsibility with the national Caldicott Guardian to ensure that the strategic implications of IG issues for NHS

¹² See section 2.4 for a summary of NHS England's statutory functions in relation to information governance

England in relation to its ability to fulfil all of its functions and duties are understood by the Board. The national SIRO chairs the National IG steering group.

3.3.3 Deputy SIROs

Deputy SIROs undertake the general roles and responsibilities of a SIRO but at a regional level / central team level and escalate any risks/issues to the national SIRO as shown in the risk management process embedded in Appendix F .Deputy SIROs are responsible for approval of privacy impact assessments and risk assessments for regional assets.

Deputy SIROs chair their region IG operational groups/ central team IG operational group and attend the National IG steering group.

3.3.4 CSU and CCG SIROs

CSU SIROs are responsible to NHS England's SIRO for IG and cyber security compliance. CCG SIROs are also responsible to NHS England's SIRO for compliance with:

- (i) operating to mandated IG and cyber security standards; and
- (ii) assuring their commissioned service providers, are operating to mandated IG and cyber security standards

These responsibilities are shown in further detail at Appendix D.

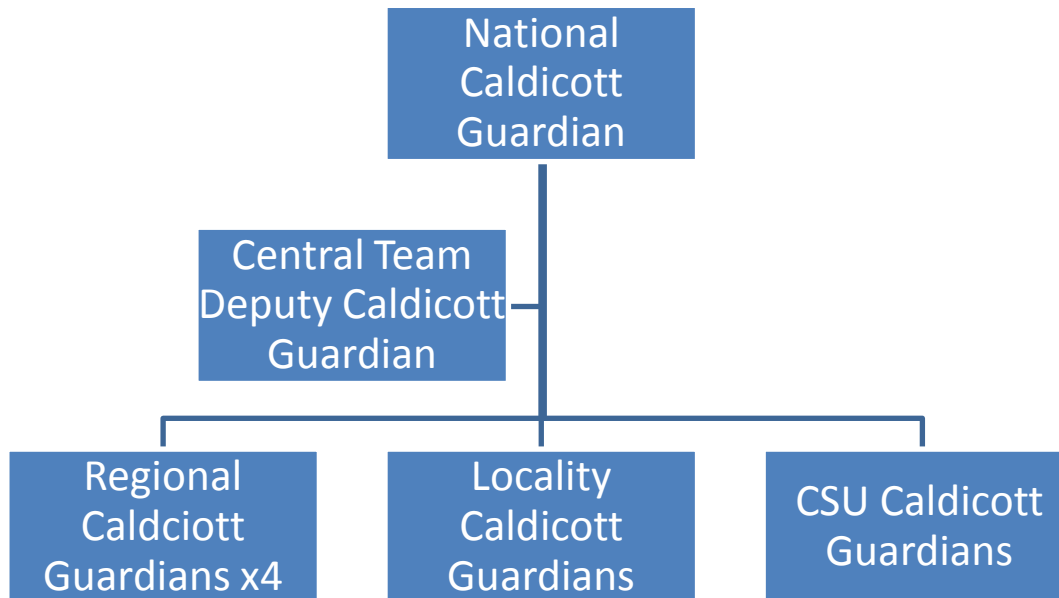
3.3.5 SIRO Training

A SIRO should possess the necessary knowledge and skills to undertake their role effectively. To support this, information risk management training should be undertaken at least annually to demonstrate their skills and capabilities are up to date and relevant to the needs of the organisation and to ensure they remain effective in their role.

More information on the roles and responsibilities of the SIRO, including training and guidance available can be found in the [NHS Information Risk Management: Good Practice Guidance](#)

3.4 Caldicott Guardians

3.4.1 NHS England's Caldicott Guardian framework



The Medical Director has been appointed as NHS England's national Caldicott Guardian. As NHS England is a very large organisation, Caldicott Guardians have also been appointed in regional teams, locality teams and in CSUs. These Caldicott Guardians are accountable to the Medical Director as Caldicott Guardian for NHS England as a whole.

3.4.2 National Caldicott Guardian

The national Caldicott Guardian undertakes the roles as described in the [Caldicott Guardian Manual](#). This includes approving data sharing agreements/ data processing agreements for national systems that contain patient data, authorising regional and locality Caldicott Guardians to be registered with NHS Digital.

The national Caldicott Guardian or his representative attends the National IG Steering Group.

3.4.3 Regional and Locality Caldicott Guardians

The regional and locality Caldicott Guardians undertake the general roles of a Caldicott Guardian at a regional or locality level. The Caldicott Guardians are key stakeholders in privacy impact assessments where there is any processing of patient data and they are responsible for the approval of information sharing agreements / data processing

agreements that contain patient data. The Caldicott Guardians will be required to approve local information disclosure requests. A Caldicott log must be maintained to ensure consistency across the organisation.

The regional Caldicott Guardians will attend their region IG operational group and the National IG steering group. The locality Caldicott Guardians attend their local IG group. The Caldicott Guardians also raise issues via the Medical Directors meetings which are held on a weekly basis and chaired by the national Caldicott Guardian. Corporate IG will work with the Caldicott Guardian to determine additional ways of supporting the regional and locality Caldicott Guardians.

Caldicott Guardians are required to undertake the e-learning training modules available: “The Role of the Caldicott Guardian: NHS and Social Care”, which provide more detailed information on all aspects of the Caldicott Guardian role. These modules are available at: <https://www.igtt.hscic.gov.uk/igte/index.cfm>

3.4.4 The differences between a Caldicott Guardian and a SIRO

Both Caldicott Guardians and SIROs play a vital part in ensuring NHS data is protected and not comprised in any unlawful and unfair manner. There is often confusion as to the difference between the SIRO and Caldicott Guardian role. The table below shows the differences between these roles:

The SIRO Is accountable Fosters a culture for protecting and using data Provides a focal point for managing information risks and incidents Is concerned with the management of all information assets
The Caldicott Guardian Is advisory Is the conscience of the organisation Provides a focal point for patient confidentiality & information sharing issues Is concerned with the management of patient information

There is clearly a need to ensure that the SIRO and any organisational Information Asset Owners work closely with the Caldicott Guardians and consult with them, where appropriate, when conducting information risk reviews for assets which comprise or contain patient information.

3.5 IG Groups

A National IG Steering group (NIGSG) has been established to support and drive the broader IG agenda. NIGSG provides the Board with the assurance that effective IG best practice

OFFICIAL

mechanisms are in place within the organisation including that an effective Records Management methodology is implemented.

This IG steering group is the overarching group responsible for the overview and scrutiny of IG arrangements across NHS England, including its hosted bodies i.e. CSUs.

In addition to this group, there are also operational IG Groups that feed into the national group:

- Central Team Operational IG Group;
- Region operational IG groups;
- CSUs IG operational groups;
- Specific Programmes/ Projects e.g. Primary Care Support England IG group

See Appendix E for terms of reference for the groups.

There are a number of other strategic, system-wide IG Groups and stakeholders which the DSPU develop and maintain relationships with such as:

- NIB Domain J
- Department of Health (DH)
- NHS Digital
- NHS Improvement
- The IG Alliance (IGA)
- The UK Council of Caldicott Guardians (UKCCG)
- The Health and Care Cyber Security Leadership Forum (CSLF)
- Care Quality Commission (CQC)
- Information Commissioner's Office (ICO)

DSPU are responsible for communicating information and issues associated with the above and where appropriate referring decisions required by those groups to the NIGSG.

Work is underway to define and align the relationships between the above groups.

4 Key Stakeholders

4.1 Department of Health (DH)

The Department of Health (DH) has government prerogative powers to produce advice and guidance to the system and overarching responsibility for ensuring that the health and social care system operates effectively as a whole. They are responsible for ensuring an appropriate legal framework is in place that supports public bodies in fulfilling their statutory functions. In the context of data this means ensuring organisations can access the data they require to fulfil their obligations, whilst also minimising the use of and protecting personal and confidential information. Alongside this system-wide responsibility, under the Health and Social Care Act 2012, the DH has specific responsibility for public health and social care,

although the delivery of many of these functions are delegated to NHS England and local authorities respectively.

4.2 National Information Board

The role of the National Information Board (NIB) is to put data and technology safely to work for patients, service users, citizens and the professionals who serve them. The NIB brings together national health and care organisations from the NHS, public health, clinical science, social care and local government, along with appointed independent representatives to develop the strategic priorities for data and technology.

The purpose of the NIB is to:

- provide leadership across health and care organisations on information technology and information
- design and develop the vision, strategy and direction for the health and care system through engagement with partners and stakeholders, including industry
- ensure that priorities for investment and delivery are clear
- provide the annual commissioning priorities for NHS Digital and turn these into an agreed delivery plan

The NIB domains are listed in Appendix A.

4.3 NHS Digital

NHS Digital has statutory responsibility to collect, analyse and disseminate health and social care data on behalf of the DH, NHS England and other bodies. It is responsible for:

- producing a code of practice for organisations processing data for uses other than the direct care of individuals
- providing advice on such processing to organisations seeking data from the NHS Digital and others seeking such advice
- the Cyber Security programme
- the IG Toolkit, including the Serious Incidents reporting tool and IG Training Tool

NHS Digital has two groups with an IG remit to support its work: the Data Access Advisory Group to act as a gatekeeper for access to Hospital Episode Statistics (HES) and the Independent Advisory Group which oversees the GP Extraction Service. NHS Digital hosts the Caldicott Implementation Monitoring Group, which has been established to monitor the performance of organisations in delivering the government commitments in relation to the Caldicott Review recommendations. NHS Digital also hosts the Information Governance Alliance.

4.4 Information Governance Alliance (IGA)

NHS England is a partner in the IGA whose mission is to enhance the quality of health and care services, including people's experience of using those services, by improving IG. The IGA aim to improve IG in health and care by:

- becoming the authoritative source of advice and guidance
- providing support to organisations to help them and their staff handle personal information confidently and in the best interests of people who use their services
- developing the leadership and culture of health and care services to promote legal and secure information sharing, and

- developing the capacity and capability of IG professionals, by providing expert advice and supporting knowledge sharing networks.

4.5 Information Commissioner's Office (ICO)

The ICO is the UK's independent regulatory body for data protection. They hold the register of Data Controllers, provide advice and guidance to organisations and the public, championing information rights and when necessary take appropriate enforcement action. They have powers to levy fines of up to £500,000.

The ICO may:

- serve information notices requiring organisations to provide the ICO with specified information within a certain time period;
- issue undertakings which commit an organisation to a particular course of action in order to improve its compliance;
- serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- conduct consensual assessments (audits) to check organisations are complying;
- serve assessment notices to conduct compulsory audits to assess whether processing of personal data follows good practice;
- issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010
- prosecute those who commit criminal offences under the Data Protection Act; and
- report to Parliament on issues of concern.

NHS England is keen to develop the ICO as critical friend by involving them in any projects and initiatives which require technical input at an early stage of development. The DSPU and Corporate IG team have regular contact with the ICO.

The ICO are an integral part of the NHS Serious Incidents Requiring Investigation (SIRI) reporting process and are notified, at the same time as the Department of Health, of any Level 2 or above SIRIs reported.

4.6 Commissioning Support Units (CSUs)

CSUs provide a wide range of commissioning support services that enable clinical commissioners to focus their clinical expertise and leadership in securing the best outcomes for patients and driving up quality of NHS patient services. This includes transformational change such as overseeing the reconfiguration of local services, transactional support including IT, HR, Information Governance and business intelligence. They provide these services to a range of customers including Clinical Commissioning Groups (CCGs), acute trusts, NHS England, and local government.

CSUs are individually autonomous and self-sufficient organisations which are hosted by NHS England. They are required to follow NHS England's overarching IG policies although they can create their own local procedures to ensure that good IG practice is embedded within their organisation.

Whilst mainly operating in the role of data processors in the provision of services to commissioners and other organisations, the CSUs operate under the Data Protection notification of NHS England for their own records.

4.7 Clinical Commissioning Groups (CCGs)

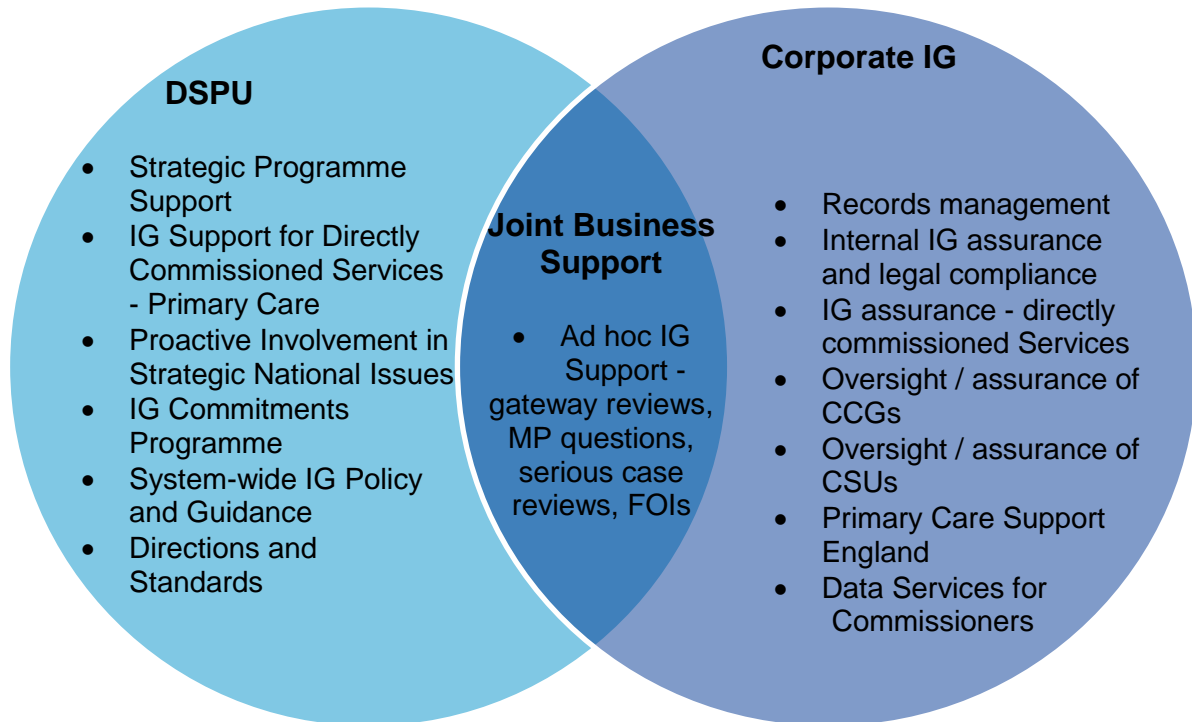
CCGs are clinically-led, statutory NHS bodies responsible for the planning and commissioning of health care services for their local area. In April 2013, they replaced primary care trusts as the commissioners of most services funded by the NHS in England. They control around two-thirds of the NHS budget.

Each CCG has a constitution and is run by a governing body which oversees and makes decisions on the delivery of its commissioning responsibilities. Each has an accountable officer responsible for ensuring the CCG's duties, functions, finance and governance responsibilities are carried out effectively, efficiently and economically.

NHS England has a statutory duty to conduct an annual performance assessment of each CCG. For 2016/17 NHS England has introduced a CCG Improvement and Assessment Framework which will be used to assess CCGs, as well as provide a focus on support to drive the improvement and transformation necessary to deliver the Five Year Forward View.

5 IG Activity Areas

- 5.1 NHS England's IG service comprises of activity areas shown in the diagram below. These activities are delivered by either the Data Sharing and Privacy Unit (DSPU) or the Corporate IG team or jointly by both teams.



5.2 The following section of this operating model will describe how each of the above activities is undertaken. The activities have been allocated a lead team of either DSPU or Corporate IG team although it should be noted that there some activities require input from both teams.

5.2.1 Ad- hoc IG Support	Provided by: Corporate IG/ DSPU
---------------------------------	----------------------------------------

DSPU and Corporate IG respond to internal requests for advice and guidance directly and as soon as possible. We aim to deliver a high degree of customer service, ascertaining what is required from the beginning and presenting achievable timelines.

The two IG teams have a joint mailbox where all ad hoc enquires should be directed. The business support function will allocate all enquiries to the appropriate team to action. The business support staff will provide cover across both teams e.g. for minute taking, hotel and train bookings, mailbox monitoring etc. Both teams will be working closely together to develop the business support function, investigate joint workflow management etc.

All queries received are systematically logged, prioritised and actioned before going through a quality assurance process to ensure consistency of approach and advice. An example of such requests include; parliamentary responses, FOI requests and clinical audit guidance.

It should be noted that both teams have limited resources and therefore it is important that risk assessments / privacy impact assessments are undertaken at the start of a project that involves any new use of data, or change to a use of data, and IG are contacted as early as possible for any advice or guidance.

Occasionally the two IG teams work closely together to produce joint documentation. This can be evidenced recently by investigating and completing an IG Assurance System MoU for the Welsh government on behalf of NHS England.

Ad hoc general IG advice and guidance is provided by both teams and responsibility has been allocated as below:

1. **General IG advice and guidance**

Enquiries, including FOI s and MP questions, should be directed to england.ig@nhs.net

This mailbox is monitored on daily basis by the Business Support team. Staff located in regional/ local teams should contact their regional IG lead/ local team IG officer as appropriate.

The Business Support team will allocate the enquiries to the appropriate team.

The Corporate IG team also develop and maintain an IG Intranet page on SharePoint which contains useful IG and records management one page guides, designated pages on information asset management, incident management and IG training, as well access to IG meeting documents. There is also access to IG published documents including IG policies and procedures. The IG intranet page is available [here](#). The site will link to the DSPU intranet site that is currently under development.

OFFICIAL

The Corporate IG team also develop regular awareness articles via Engage and SharePoint headlines. There is also a records management newsletter 'For the Record' that is sent out to local Records Management Coordinators. Records Management Coordinators have been identified across the organisation and they support and cascade good records management practice to their wider teams (for further information [click here](#)).

DSPU provide input and write articles for the both the IGA and the ICO monthly newsletters.

An internal DSPU and Corporate IG newsletter is in development.

2. Provision of IG advice and guidance to NIB Domain programmes and other projects

All enquiries should be directed to the generic mailbox as in section 1 above.

Where requests are for complex tasks or for project/programme support, a Project Outline Document (POD) is completed by the customer, which identifies budget, stakeholders, timescales, etc. The DSPU will then ascertain what level of commitment and resources are needed and work closely with the customer to meet their IG requirements. This document will be accessible digitally on our own dedicated DSPU intranet page in the near future. This page will also provide useful information such as Privacy Impact Assessments advice and FAQs.

DSPU are also tasked with answering external requests, including those originally sent to IGA, but require a response from NHS England.

DSPU provide strategic IG advice and guidance for Digital roadmaps. However there may be other requirements for IG advice and guidance e.g. Privacy Impact Assessments, data sharing, procurement etc. that are considered to be business as usual and therefore a corporate IG responsibility. This may cause resourcing issues in the near future for the Corporate IG team.

3. Serious case reviews (SCRs)

Serious case reviews may relate to a single provider or involve multiple providers. There is a need for adequate IG resource to support serious case reviews, to ensure independence of decision-making. This support will be provided by the Corporate IG team and enquiries should be made to england.ig@nhs.net.

4. Gateway reviews

Gateway clearance for documents with IG implications will need to be sent to england.ig@nhs.net for IG approval. The Business Support team will screen the mailbox and any NHS England internal documents will be assessed by the Corporate IG team for

approval. External documents (e.g. guidance for CCGs, GPs) are reviewed and approved by DSPU.

5. Consultations

DSPU are relied upon to provide input to NHS England responses, for any government or other public consultations which have an IG component.

Mostly, the requirement is for DSPU input into a final response, drafted by other departments. However, occasionally the unit will be asked to lead on the collation and publication of the response, such as the HES Privacy Impact Assessment consultation.

6. Information Governance Alliance (IGA) Liaison

A high volume of documents drafted by others and coordinated by the IGA require input and comment from NHS England. DSPU identify relevant internal key stakeholders and liaise with them in order to provide IGA with a full and robust response to any guidance. The DSPU identify those whose input is required. As part of that process they involve Corporate IG and where relevant, ask for their participation to review and comment.

The DSPU consider, collate and provide a response to IGA team on behalf of NHS England.

5.2.2 Strategic Programmes Support	Provided by: DSPU
-------------------------------------------	--------------------------

IG support for strategic programmes is provided by DSPU.

Some programmes which fall outside of the NIB domains require IG input. (See Appendix A).

DSPU looks to the NHS Five Year Forward View (FYFV) to ensure that the projects and programmes of such initiatives have IG consideration.

One of their key tasks is to highlight the need to ensure that programmes understand that privacy should be considered at the beginning of a project, through completing a Privacy Impact Assessment. This ensures that risks to privacy are identified and alleviated.

A substantial amount of the work involves input into new projects programmes and initiatives. Some of these require minimal input to ascertain IG requirements and then hand over to the project team themselves. Others require more in-depth and detailed work plans, to ensure proper consideration, and actions are put in place and followed with regard to IG. The promotion, development and consideration of Privacy Impact Assessments are key to this process.

Provision of support is usually provided internally within DSPU. In the past, work has been outsourced to contractors who would provide support and guidance, but this practice is costly and inefficient and therefore in future will no longer take place. DSPU works closely with the programmes and contractors. If applicable, they advise upon the IG resources and

requirements. An example includes working with Interoperability/Digital colleagues, in relation to presenting advice on the development of the Direct Care Model for data sharing.

1. Post programme business as usual

DSPU has responsibility to support strategic programmes and projects during their lifespan, and it will be the responsibility of the business area to maintain IG conformance. The ongoing IG support for the business areas should be provided by Corporate IG team, who will develop a formal hand-over process for programmes that are completed. These need to be handed over to Corporate IG team as 'business as usual'. The handover should be comprehensive and ensure that all business as usual requirements have been considered, including resources required to provide ongoing IG support.

<p>5.2.3 IG Support for Directly Commissioned Services – Primary Care</p>	<p>Provided by: DSPU</p>
----------------------------------------------------------------------------------	---------------------------------

1. NHS England's Responsibilities for GPs

GPs are data controllers in their own right and are therefore responsible for compliance with all necessary laws and IG standards. However, NHS England has a responsibility as a commissioner to ensure that GPs operate appropriately. NHS England also has an ethical and moral duty to ensure that those organisations it commissions, handle patient information in a secure and legitimate manner. To assist this, a GP IT Operating Model has been developed to describe the arrangements that should be in place. The extract below demonstrates the main purpose of this document.

2. IG Support for GPs (extract from GPIT Operating Model 16-18)

NHS England is accountable for the delivery of GP IT services, delegating responsibility for delivering key elements of GP IT services to clinical commissioning groups (CCGs). These arrangements promote equity and ensure a consistent core offer in all parts of the country. This gives General Practices the flexibility to meet local needs within a nationally agreed framework, whilst adhering to national IG and security standards which are underpinned by a centrally managed, assurance process.

NHS England retains responsibility for commissioning services to support all Primary Care Contractors offering Primary Care Enabling Services to a registered patient list, to fulfil their statutory responsibilities relating to IG and to support compliance with the IG Toolkit (IGT).

NHS England will commission local services to support adherence to IG policies and procedures and provide support for the completion of General Practice IGT submissions.

A Commissioning Specification: 'Information Governance Support for Primary Care Providers' has been developed to deliver an outline structure for contracting purpose and inform NHS England's Regions about the IG support that they must commission for Primary Care providers.

3. Key Principles:

- NHS England will set national IG policy
- NHS England will ensure that the provision of a local IG support service for Primary Care contractors, including appropriate support for the management of IG and Information Security incidents.
- All parties are accountable for their compliance with all necessary IG laws and standards.

4. IG responsibilities:

- DSPU are responsible for the development of the IG support service specification.
- The Heads of Digital Technology, within the regional teams are responsible for ensuring a service is commissioned.

5.2.4 Proactive Involvement in Strategic National Issues	Provided by: DSPU
-----------------------------------------------------------------	--------------------------

The overall aim is to ensure that DSPU has an awareness of what is on the horizon and therefore can ensure they feed into key national strategies and initiatives. These include contributing to reviews and involvement on panels which deal with specific national initiatives, such as the National Data Guardian Review, Devolution Manchester, the General Data Protection Regulations etc.

These areas of work are shown in our business plans, as key items.

5.2.5 IG Commitments Programme	Provided by: DSPU
---------------------------------------	--------------------------

External changes are addressed within the DSPU.

The term ‘external system change’ relates to un-anticipated changes which arise from external factors such as political, economic, social, technological and legal.

To that end, an IG Commitments programme has been introduced which will include the impacts of the National Data Guardian Review.

5.2.6 System Wide IG Policy and Guidance	Provided by: DSPU
-------------------------------------------------	--------------------------

There are three strands of work associated with the planning and delivery of our work for the Information Governance Alliance:

Commissioning Guidance – where we believe guidance is required for national level awareness, we may decide to use the IGA commissioning process, by submitting a detailed report about what is required, the target audience and timescales. Presentation of the suggestion must be undertaken.

Drafting Guidance – the IGA may request the DSPU drafts guidance, which they have asked to be commissioned. They may also request that we draft guidance commissioned by others. In this scenario we have responsibility for taking the guidance through the discussion, consultation and sign off process.

Endorsement of Guidance – the DSPU may produce guidance which requires endorsement from the IGA. In this case we are required to present the guidance to the IGA Editorial Panel.

DSPU also liaise with the IGA in relation to answering enquires.

DSPU are represented on the Programme Board, the Editorial Board and at the Management meetings.

5.2.7 Directions and Standards	Provided by: DSPU
---------------------------------------	--------------------------

DSPU have responsibility for the consideration and drafting of Directions Required for instructing NHS Digital, to require certain data for specific circumstances. It involves the team following due process and assisting programmes through the process.

The unit also has responsibility for assisting with the identification, development and implementation of certain standards.

DSPU are also responsible for ensuring changes to legislation which impact upon IG, are recognised. Raising awareness to the wider system about these changes, sits in DSPU remit.

5.2.8 Records Management	Provided by: Corporate IG Team
---------------------------------	---------------------------------------

Records Management advice and guidance is provided by the Records Manager and the Records Management Officer, within the Corporate IG team. The Records Manager is responsible for maintaining the NHS England Document and Records Management Policy and the NHS England Retention and Disposal Schedule and Guidance, ensuring that the schedule reflects external policy in the public sector.

Records Management guidance is provided for all staff via the intranet, including the creation, maintenance, storage and disposal of records within NHS England. A bespoke,

OFFICIAL

online Records Management Training package has been provided for all staff and this is available within the [Learning Management System](#).

Records management queries can be received verbally, via telephone or via email (england.ig@nhs.net) and these are responded to, as soon as possible. All queries are maintained in a database for future reference and referral.

The Records Management team have responsibility for promoting the use of the Electronic Records Management System (ERMS), which is located on the NHS England intranet. Having just been launched in August 2016, the ERMS is the repository for all NHS England records and is in the process of being embedded.

Records Management is a work stream within the Information Management Programme at NHS England. The Records Manager leads on the records management work stream and feeds into regular meetings of the Operational Information Management Group.

An inventory is maintained of the legacy archive which is held by NHS England. This archive was inherited from the Department of Health and consists of records from the closed Primary Care Trusts (PCTs) and Strategic Health Authorities, which existed before April 2013. The team receive numerous queries and Freedom of Information requests about legacy records and maintains a database of these queries.

Regular audits are undertaken in accordance with the Information Management Audit Framework. The audit framework covers confidentiality, records management and data quality. These audits are undertaken by the central team and the regional/ locality teams.

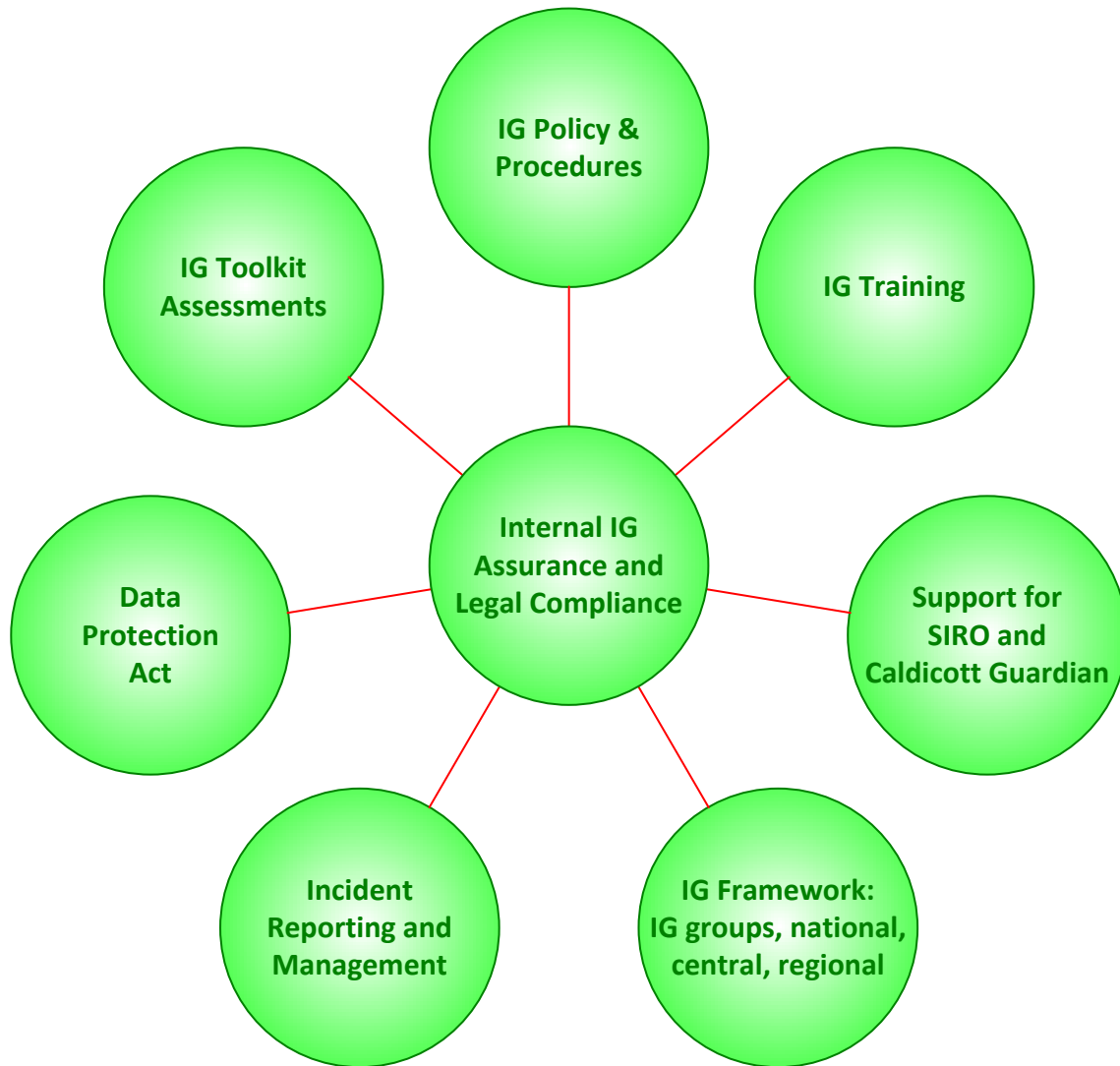
Records Management Co-Ordinators (RMCs) have been established across the organisation. They are responsible for promoting records management within their locality, cascading advice and guidance to members of their teams, undertaking Records Management Training and uploading corporate records to the Electronic Records Management System (ERMS).

There is a bi-monthly meeting with RMCs, which is delivered via webinar. This meeting informs RMCs about the latest developments in records management and also offers an opportunity for RMCs to discuss local issues with colleagues. The terms of reference for the group can be found in Appendix E. In addition to the meetings, a quarterly bulletin for RMCs is produced, advising them of the latest news, in terms of records management activities and planned developments.

Induction is provided for every RMC and they are also expected to complete the online Records Management Training as a mandatory part of their role – for other NHS England staff, this is optional. An online Yammer group for RMCs has recently been established and this will further promote good records management within NHS England.

5.2.9 Internal IG Assurance and Legal Compliance	Provided by: Corporate IG Team
---------------------------------------------------------	---------------------------------------

NHS England’s internal IG assurance and legal compliance is provided by the Corporate IG team. The main activities include:



The above activities are undertaken across the Corporate IG team, including regional and local teams. The breakdown of responsibilities is shown in more detail in Appendix F. Each listed activity also shows the relevant policy/ procedure for further information, and the IG Toolkit reference where appropriate. Appendix G shows the Corporate IG team objectives for 2016-17.

5.2.10 IG Assurance for Directly Commissioned Services	Provided by: Corporate IG Team
---------------------------------------------------------------	---------------------------------------

1. Primary Care - IG Assurance and Levers

IG Toolkit
<p>NHS England sets the requirements to be included in the IG Toolkit (IGT) as a standard, and commissions NHS Digital to deliver the tool.</p> <p>GP practices, under the GPIT operating model 16-18, are responsible for completion of the IG Toolkit and attainment of Level 2 compliance, with support from their IG Support Service.</p> <p>Under S250 of the Health and Social Care Act, GPs are required to have regard to the standards that NHS England sets and the IGT is one of these standards.</p> <p>Compliance with the IGT is also mandated for all organisations that have an N3 connection.</p> <p>NHS England Regional teams are required under the GPIT operating model 16-18 to monitor compliance in their area.</p> <p>The Primary Care web tool provides the status of IG Toolkit compliance for each GP Practice. Corporate IG will work with commissioning operations to determine a process for monitoring compliance and targeting GPs where necessary, as part of the contract monitoring process. Reports will be provided to the NIGSG.</p> <p>The ICO will also provide a monthly report to Corporate IG team, detailing any GP complaints/ investigations, for dissemination to the relevant commissioning team.</p> <p>It is recognised that the IG Toolkit is self-assessment and there is currently no requirement for an independent audit to be undertaken. NHS England will explore the feasibility of commissioning audits, where there are significant concerns.</p>
IG Support Services
<p>DSPU have developed a Commissioning Specification: Information Governance Support for Primary Care Providers to inform NHS England's Regions about the IG support that they must commission for Primary Care providers, and provide an outline structure for contracting purposes.</p> <p>NHS England Regional Teams are responsible for commissioning a local IG support service as outlined in the above specification and funding has been provided for this.</p>
Reporting IG Serious Incidents Requiring Investigation (SIRIs)
<p>NHS England, under the GPIT operating model 16-18, is accountable for investigating and</p>

taking appropriate action relating to all Serious Incidents Requiring Investigation (SIRIs), relating to information security and other data breaches.

NHS England, under its responsibility for standards, sets operational policies and procedures relating to SIRIs, develops SIRI reporting requirements in the IG toolkit and STEIS (STrategic Executive Information System) and oversees governance of SIRIs.

GPs are required to report any IG breaches via the IG Toolkit as per the standard. They are also required to report SIRIs to their commissioner as part of the contract.

NHS England Region/ Locality Teams are responsible for commissioning a service to investigate SIRIs, as part of the GPIG service specification.

NHS Digital provides a full report of all SIRIs on a monthly basis.

SIRI is part of the DSPU IG Commitments Programme for 16-17 and recommendations will be produced shortly.

Contracts

The GMS Contract 16/17 (General Medical Services) provides the following assurance :

NHS England and the General Practitioners Committee will continue to promote the completion of the IG toolkit, including adherence to the requirements outlined within it.

Practices will also continue under the GMS Regulations to nominate a person with responsibility for practices and procedures, relating to the confidentiality of personal data.

With the sheer volume of patient information that a GP practice handles, it is vital that practices can handle information confidentially and securely, and that they can demonstrate this.

Practices should also be cognisant of the National Data Security Review recommendations that will outline a set of recommendations and data security standards, including the potential subsequent iteration of the IG toolkit.

Cyber Security

Assurance for the Data Security Standards is currently provided by compliance with the IG Toolkit (IGT).

NHS Digital are currently revamping the IGT to provide a new data standards toolkit. NHS England will work with NHS Digital to ensure that cyber standards in the new Toolkit are adequate and appropriate.

Note: Corporate IG will work with Primary Care commissioning to determine what assurance needs to be provided for other Primary Care contractors e.g. dentists, opticians and pharmacies.

2. Specialised Commissioning

Specialised commissioning is currently delivered through four regional specialised commissioning teams, each having hubs, which commission specialised services at a more local level.

The regional teams manage the performance of the commissioning hubs. The commissioning hubs are responsible for the commissioning of specialised services from providers within their geographical locality and they commission on behalf of the whole country. Responsibility for the oversight of IG Toolkit compliance currently rests with the regional IG teams.

It has been identified that further work is required to understand the IG assurance mechanisms that are in place and to determine the adequacy. A business case has been developed to secure funding to enable this review to be undertaken.

3. Armed Forces Healthcare

Armed Forces Health was originally commissioned from three teams, but now it is commissioned by a single team across three bases - York, Derby and Chippenham. The Corporate IG team are currently working with this team to develop an IG assurance process.

4. Health and Justice Healthcare

The Corporate IG team are currently scoping a project to understand the commissioning responsibilities, data flows and data controllership for Health and Justice Healthcare. One objective of this work will be to ensure an IG assurance model is developed.

5.2.11 Oversight/ Assurance of CCGs	Provided by: Corporate IG team
--------------------------------------------	---------------------------------------

NHS England requires assurance that those bodies who commission services, either on their own or jointly, undertake contract monitoring to ensure providers are adhering to IG requirements. Assurance of indirectly commissioned services rests with CCGs, local authorities and lead providers.

The CCG Assurance Framework 2015/16 has been superseded by the CCG Improvement and Assessment Framework 2016/17. The 2016/17 Framework is fully aligned to the NHS England 5-year Forward View and NHS planning guidance and comprises 60 metrics (areas of medical programme) in 29 areas. Unfortunately the framework does not include any metrics regarding IG and therefore Corporate IG are currently investigating ways of providing IG Assurance.

CCGs are required to complete an IG Toolkit and achieve the minimum satisfactory level, as part of their Data Sharing Contracts with NHS Digital. The IG Toolkit status is to be checked annually by the Corporate IG team. NHS England is currently reviewing whether independent audits of IG Toolkit assessment are required.

There is no mechanism that requires CCGs to be responsible for holding providers to account. DSPU are responsible for statutory guidance, which can include guidance for commissioners, on how to hold such providers to account and the standards that should be met. DSPU are to produce guidance to CCGs to determine the level of IG assurance and monitoring arrangements that are required for their providers.

In addition to the above, CCGs will need to demonstrate that they are seeking assurance from their data processors that are externalised e.g. CSUs that are now private organisations. The assurance required should be detailed in the contract with the data processor. Section 5.2.12 below, shows the type of assurance that NHS England will be requesting from those CSUs that are hosted by NHS England.

5.2.12 Oversight/ Assurance of CSUs	Provided by: Corporate IG team
--------------------------------------------	---------------------------------------

1. Background

NHS Commissioning Support Units (CSUs) are hosted by NHS England. They are required to follow NHS England's overarching IG policies, although they can create their own local procedures to ensure that good IG practice is embedded within their organisation.

Whilst mainly operating in the role of data processors in the provision of services to commissioners and other organisations, the CSUs operate under the Data Protection notification of NHS England for their own records.

NHS England provides oversight and assurance of IG Toolkit returns from CSUs. It manages CSU compliance of the overarching policies by monitoring incidents and engaging on a regular basis with CSU IG Leads, via the IG Leads meetings and the National IG Steering Group (NIGSG).

Oversight and assurance of private organisations undertaking CSU services, is the responsibility of the CCGs that commission their services. This are covered in more detail in section 5.2.11 of this operating model.

2. CSU IG Assurance

Oversight and assurance of CSUs is provided by the following:

- Governance and Assurance meetings – undertaken twice yearly by the CSU Transition Team – (for responsibility description see section 4.1)
- Monthly assurance statement, contained in dashboard returns – signed by CSU managing director
- Annual Independent Audit
- Reports to Corporate IG team
- CSU IG leads group

OFFICIAL

IG requirement:	CSU responsibility:	NHS England responsibility:
Roles and Responsibilities	<p>Appoint the following roles and ensure Corporate IG are kept up to date:</p> <ul style="list-style-type: none"> • Appoint a local SIRO • Appoint a local CG • Establish a local IG group • Provide a representative for NIGSG 	<p>To be checked by the governance and assurance meetings undertaken by the CSU Transition Team. (see part 4 below).</p>
IG Policies	<p>A monthly assurance statement is signed by the managing director to confirm that the CSU is compliant with key NHS England policies including:</p> <ul style="list-style-type: none"> • Information Security • Information Governance • Information Sharing • Document and Records Management • Corporate Records Retention and Disposal Schedule and Guidance 	
IG Training	<p>Ensure staff are required to undertake IG training which is aligned with NHS England training needs analysis.</p>	<p>To be checked by the governance and assurance meetings by the CSU Transition Team.(see part 4 below).</p>
IG Toolkit Assessments	<p>Undertake own IG Toolkit assessment. Confirm to Corporate IG when baseline, interim, and final assessments are completed. To provide a copy of the action plan to Corporate IG team and provide quarterly update reports highlighting any exceptions.</p> <p>Forward a copy of the Internal audit report to Corporate IG.</p>	<p>To monitor compliance and include in NHS England's annual governance statement.</p> <p>To escalate risks to SIRO as appropriate.</p> <p>CSU Transition Team to commission independent audit of the IGT assessment.</p>
Information Assets	<p>Appoint IAOs/IAAs and maintain own information asset register.</p> <p>All information assets should be identified and categorised to indicate the level of PCD contained within them and the associated controls to restrict access to the asset.</p>	<p>To be checked by the governance and assurance meetings undertaken by CSU Transition Team. (see part 4 below).</p>

OFFICIAL

<p>Contracts/ Data Processing Agreements</p>	<p>CSUs will maintain their own contracts register and data processing agreements register.</p> <p>CSUs are data processors acting on behalf of the commissioners they are contracted to provide support services for. The CSUs cannot enter into data sharing agreements with other organisations. CSUs will need to ensure that CCGs have a service level agreement and/or a data processing agreement in place to support their data processing activities and can demonstrate compliance with DPA 7th principle.</p>	<p>To be reviewed by the independent audit of the IG Toolkit.</p> <p>Corporate IG to undertake an annual check to ensure all CSUs have appropriate contracts in place to support their data processing activities with each CCG.</p> <p>NHS England are responsible for ensuring CSUs are compliant with conditions for processing under s251 for risk stratification and invoice validation. Each CSU is required to sign an assurance statement that the relevant controls are in place.</p>
<p>Caldicott Issues Log</p>	<p>Caldicott issues log should be maintained.</p>	<p>Review for consistency in the CSU IG leads group.</p>
<p>IGT Compliance Audits</p>	<p>Conduct IG compliance audits as required by the IG toolkit.</p>	<p>To be reviewed by the independent audit of the IG Toolkit.</p>
<p>Risks and Issues- Escalation</p>	<p>The CSU should maintain their own risk management system.</p> <p>High risks and issues should be escalated to the CSU Transition Team.</p>	<p>The CSU Transition Team have a risk register, hold a monthly risk meeting to review all CSU related risks and operational risks are reported to the SIRO at the CSU Operational Risk Group (CORG).</p> <p>Details of any IG risks are provided to the Corporate IG team for inclusion on the Corporate IG risk register.</p> <p>Any high risks/issues would be escalated</p>

OFFICIAL

		directly to the SIRO via the Corporate IG team if deemed appropriate.
Security Incident Reporting and Management	<p>CSUs will investigate and report incidents as per the incident reporting procedure. This requires all incidents to be recorded on NHS England's system or a local reporting system. SIRIs should be escalated to the central team IG lead (within 24 hours) prior to reporting via the IG toolkit incident reporting system. Lessons learned should be disseminated throughout the CSU.</p> <p>Details of all incidents should be provided to Corporate IG on a monthly basis as stated in the information security incident reporting procedure.</p>	<p>Appropriate IG lead to agree SIRI level to enable the CSU to report via the IG Toolkit where required.</p> <p>To include incidents in the monthly performance reports and annual governance statement.</p>
DPA Notification	CSU processing is included in NHS England's DPA notification and therefore CSUs must inform Corporate IG of any new information processing of personal data. Any processing outside the UK must be approved by NHS England and notified to the Corporate IG.	To be checked by the governance and assurance visits undertaken by CSU Transition Team. (See part 4 below).
DPA: Subject Access Requests	<p>To complete any SAR requests.</p> <p>Provide a quarterly report to Corporate IG.</p>	Include SAR figures in quarterly reports for the Central Team Operational IG Group.
ICO Investigations	Provide support to Corporate IG as appropriate.	Manage any ICO investigations with support from the CSU.
Records Management	<p>CSUs must follow NHS England's Document and Records Management policy and Retention and Disposal Schedule.</p> <p>Destruction certificates to be sent to NHS England's record manager.</p>	Records management audits checked by the independent audit of the IGT.

3. Region IG Groups

CSUs may access the Region IG groups to discuss local issues. The following shows the relevant region group for each CSU:

CSUs	Region IG Group
Arden & Greater East Midlands CSU	Midlands & East
Midlands and Lancashire CSU	Midlands & East
North & East London CSU	London / Midlands & East
North of England CSU	North
South, Central & West CSU	South
South East CSU	London

4. CSU Transition Teams

4.1 The CSU Transition Teams are responsible for completing the following audit checklist, twice yearly in each CSU

Activity:	Compliance Check:	Comments:
Roles and Responsibilities	Confirm that the CSU has <ul style="list-style-type: none"> • Appointed a local SIRO • Appointed a local CG • Established a local IG group • Provide a representative for NIGSG 	
IG Training	Ensure IG training provided to staff, is either the IG Training Tool or equivalent. Review evidence of monitoring of staff training.	
Data Protection	Check that NHS England's DPA notification covers the processing undertaken by the CSU and that any processing outside the UK has been approved by NHS England.	
Information Assets	Check that IAOs and IAAs have been appointed for information assets and that they are recorded appropriately in the Information Asset Register.	
Internal Audit Review	Ensure an internal audit of the IGT is undertaken on an annual basis. (The transition team are currently looking at securing funding to commission NHS Digital to undertake this service.)	

5.2.13 Primary Care Support England**Provided by: Corporate IG Team**

NHS England is responsible for providing Primary Care support functions and Capita have been contracted to deliver this service. A separate IG Operating Model has been developed for the provision of these services and describes the various IG roles and responsibilities.



IG Operating Model
for PCSS - 8 Sept 201

The Corporate IG Team provide IG support and oversight to Primary Care Support England (PCSE) by monitoring their compliance with the DPA, IG Toolkit, incident management and providing ad-hoc advice on information disclosures.

There is a monthly PCSE IG Forum, co-ordinated by the NHS England Service Management Team and this group is responsible for the following:

- ensuring that there is clarity around the operational IG requirements of Primary Care Support England.
- ensuring that the IG Operating Model is updated as and when required.
- monitoring adherence with the IG Operating Model, including high level monitoring of the IG Toolkit completion.
- providing a forum for IG operational issues, to be raised by Capita, NHS England or Public Health England.
- establishing 'task and finish' sub groups for any specific IG related issues, as and when required.
- providing an overview of Capita's transformation programme and associated IG issues.
- review and feedback of Privacy Impact Assessments and other IG documents related to PCSE services.
- monitoring of IG incidents in PCSE.
- review of IG risks in PCSE.

National Health Applications and Infrastructure Services (NHAIS)

Under the revised GMS Contracts regulations¹³, NHS England is responsible for maintaining a list of patients registered with GP contractors in England. Consequently, NHS England is the primary data controller for the core registration data, within NHAIS.

This data is processed on our behalf by NHS Digital. In order to ensure that appropriate governance is in place around the processing and use of this data, the Corporate IG team have implemented an NHAIS Authorisation Board (NAB). This meets fortnightly to discuss requests and where appropriate, authorises the disclosure of national datasets from data held within NHAIS systems, or it authorises a legitimate organisational link to NHAIS data, to support direct care.

¹³ Health Service (General Medical Services Contracts) regulations 2004 [SI 2004/291] as amended by Regulation 27(8) The National Health Service (Primary Medical Services) (Miscellaneous Amendments and Transitional Provisions) Regulations 2013 See <http://www.legislation.gov.uk/ukxi/2004/291/schedule/6/made> and <http://www.legislation.gov.uk/ukxi/2013/363/regulation/27/made>

NAB includes the NHAIS Information Asset Owner, the Public Health England IG Lead, the NHS Digital System and Service Delivery Manager together with corporate IG and PCS representatives. Once agreed by the NAB members, requests are authorised by the NHS England Caldicott Guardian. If NAB members decline a request, the requestor is provided with clarification of the reasons why.

NAB also provides governance support to the PCSE team, in relation to the transfer of services to Capita.

<p>5.2.14 Data Services for Commissioners</p>	<p>Provided by: Corporate IG Team</p>
------------------------------------------------------	----------------------------------------------

The Data Services for Commissioners (DSfC) programme has been established to improve NHS Commissioning, by ensuring that commissioning decisions, and the insights that support them, are based upon robust, standardised data that has been processed efficiently and is accessed legally.

Our intention is that all staff and organisations that support or carry out NHS commissioning activities, will be fully and demonstrably compliant with the IG requirements of the Health and Social Care Act 2012 and the Care Act 2014, and will only use identifiable data when there is a clear need and stated legal basis to do so.

As this is a programme that will require a significant amount of business as usual IG processes, it was agreed that the Corporate IG team would provide the IG support for this programme.

One of the DSfC service areas is to support commissioners, so they receive the data they require to meet their statutory duties.

The support provided by the Corporate IG team extends to working with Commissioners, the Confidentiality Advisory Group (CAG), NHS Digital, and many other stakeholders. This is to help identify the legal basis upon which commissioners can receive data, and to agree specifications which minimise the level of identifiable data required.

From October 2016, commissioners will receive data which has been anonymised in accordance with the Information Commissioners Anonymisation Code of Practice, unless a specific legal basis allows the provision of identifiable data. The data specification which has been agreed with NHS Digital for commissioning purposes, is outlined in the “Data Services for Commissioners: Requirements for Data” which has been anonymised in line with the ICO’s Anonymisation Code of Practice.

The DSfC team also require specific IG support in relation to the following key areas:

- supporting NHS Digital, with the development of guidance for organisations processing data anonymised in line with the ICO Anonymisation COP, as there are wider technical and business controls which must be implemented in recipient organisations

OFFICIAL

- supporting NHS Digital in their development of a service which will enable anonymised data to be re-identified and disclosed, where a lawful and legitimate request is received
- the management of both the Risk Stratification and Controlled Environment for Finance (CEfF) registers, which are required as a condition of CAG approval, for the processing of data undertaken by CSU's/CCGs under s251 of the NHS Act 2006
- undertaking audits of CSUs, to ensure that they have the appropriate data processing agreements in place with the commissioners they are providing services to
- undertaking audits of CCGs websites, to ensure that their Fair Processing Notices information adequately informs patients about how their information is used and with whom it may be shared with.

IG support ensures that the legal risks and issues associated with the collection and provision of data to commissioners are managed appropriately, so that safe and lawful data processing can be undertaken.

6 IG Operating Model Glossary

Caldicott Guardian (CG) - a Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information, and enabling appropriate information sharing.

Confidentiality Advisory Group - the Health Research Authority's (HRA) responsibilities for the regulation and governance of health and social care research are defined in the Care Act 2014. To carry out these responsibilities in relation to data, the HRA appoints the Confidentiality Advisory Group (CAG) to provide advice on the uses of data, as set out in the legislation.

Data Protection Act 1998 - all staff working with personal data are required to comply with the Data Protection Act. The Act is summarised by eight principles of data:

1. processed fairly and lawfully
2. obtained for specified and lawful purposes
3. adequate, relevant and not excessive
4. accurate and up-to-date
5. not kept for longer than necessary
6. processed in accordance with the rights of the data subject
7. held securely
8. not transferred outside the EEA, without adequate protection

Electronic Record Management System (ERMS) - identifies that the organisation has the records it needs, when they are needed. The system manages corporate records within classification schemes, applies retention and disposal schedules, and controls access and use. It also allows NHS England to meet certain legal requirements, for example the function of applying retention periods automatically to records.

Information Asset - can be defined as operating systems, infrastructure, business applications, off-the-shelf products, user-developed applications, records and information. An information asset will have recognisable and manageable value, risk, content and lifecycles. It can range from a basic Excel spread sheet or database, to a national system.

Information Asset Administrators (IAA) - these are usually operational members of staff, who understand and are familiar with the Information Asset within their area.

Information Asset Owners - (IAO) - these are expected to understand the overall business goals of the organisation and their department, and how the information assets they own contribute to and affect these goals. They support the SIRO and deputy SIROs in managing the information risk agenda.

Information Governance - a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards, in a modern health service. It provides a consistent way for employees to deal with the many different information handling requirements.

Information Sharing Agreements (ISAs) - sometimes known as 'Information or data sharing protocols' or data sharing agreements – set out a common set of rules to be adopted by the various organisations involved in an information sharing operation. These could well form part of a contract between organisations. It is good practice to have a data sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

National Health Applications and Infrastructure Services (NHAIS) - NHAIS systems form one of the largest databases in operation in England. They were previously managed by Connecting for Health and latterly NHS Digital (formerly known as the Health and Social Care Information Centre (HSCIC)). Under the revised GMS contract regulations, NHS England is responsible for maintaining a list of patients registered with GP contractors in England. This data comprises of demographic data only and does not include any clinical information relating to patients. NHS England is the primary data controller for the core registration data, within NHAIS.

Personal Confidential Data (PCD) - this is a term used in the Caldicott Information Governance Review and describes personal information about identified or identifiable individuals, which should be kept confidential and includes dead as well as living people. The review interpreted 'personal' as including the Data Protection Act 1998 definition of personal data, but included data relating to the deceased as well as living people. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act 1998.

Privacy Impact Assessment (PIA) - a Privacy impact assessment is a process which helps an organisation to identify and reduce the privacy risks of a new process, service, information system/ asset. An effective PIA will be used throughout the development and implementation of a project, using existing project management processes.

Serious Incidents Requiring Investigation (SIRI) - is any incident involving the actual or potential loss, theft or unauthorised disclosure of person-identifiable information which could lead to identity fraud or have other significant impact on individuals (e.g. you find a confidential letter on a photocopier, or a lost or stolen NHS England laptop)

Subject Access Request (SAR) - Under the Data Protection Act (DPA) 1998 anyone has the right to see and have a copy of information about them which is held by NHS England, this is known as a Subject Access Request.

Appendix A: Strategic Projects and National Information Board (NIB) Domains

The following table shows the strategic projects and the relevant team that are providing IG support:

Topic/Programme	DSPU	Corp IG
Cyber security	X	X in conjunction with Corporate ICT
Devolution	X	X
Data Services for Commissioners		X
GDPR	X	X
National data guardian review	X	X
Primary Care support services (capita)		X
Primary Care support - GPAF	X	
Vanguards	X	
New models of care	X	
Test beds	X	
Digital roadmaps	X	

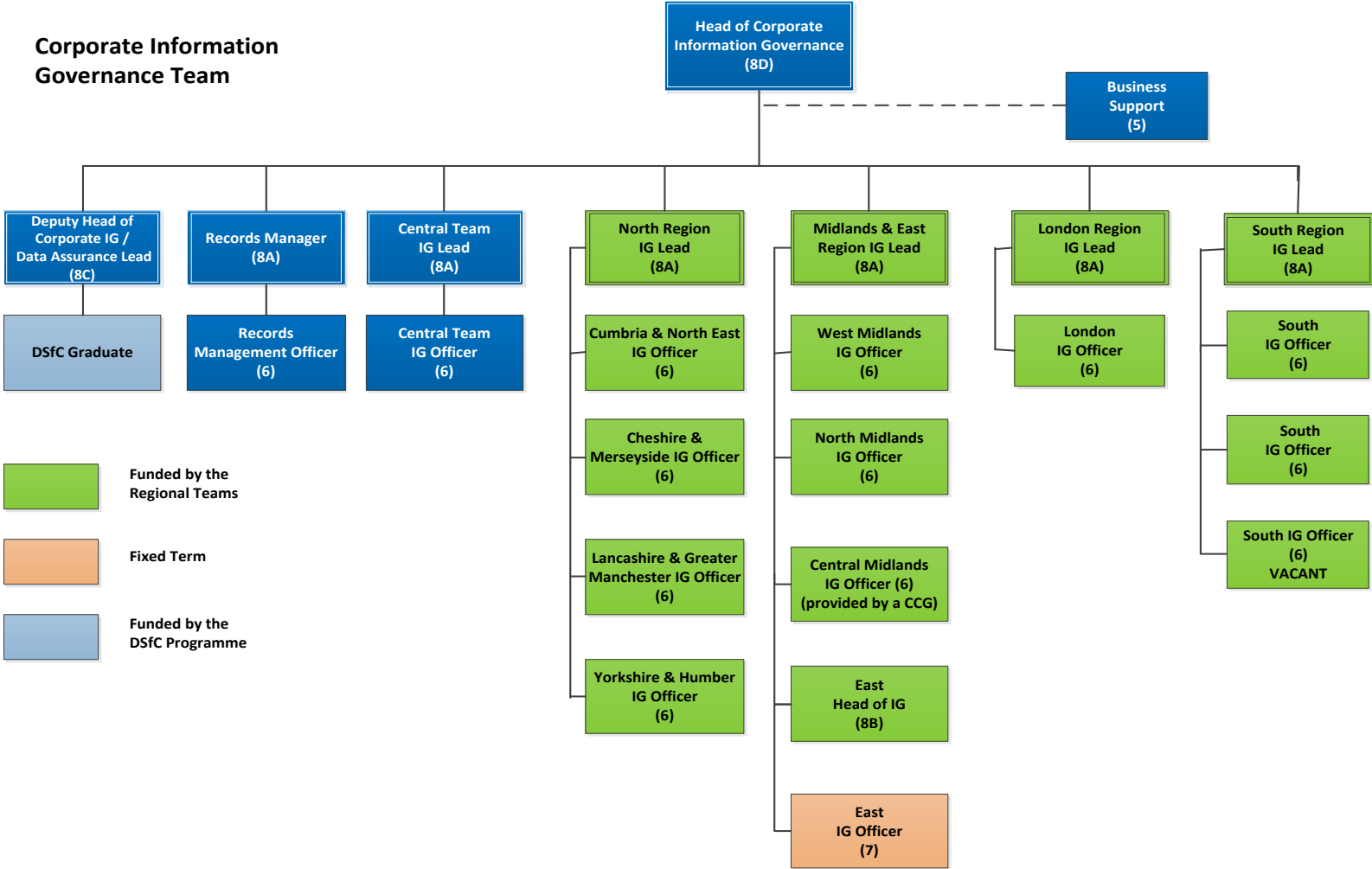
NIB Domains – Programmes assisted by DSPU to date (highlighted)

Domains	Programmes
A. Self Care and Prevention	1 Citizen Identity
	2 NHS.UK
	3 Health Apps Assessment & Uptake
	4 Widening Digital Participation
B. Urgent & Emergency Care	5 Clinical Triage Platform
	6 Patient Relationship Management
	7 Access To Service Information
	8 Out of Hospital Care
C. Transforming General Practice	9 General Practice Operational Systems and Services
	10 Adopting Existing Technologies in General Practice
	11 Technology for General Practice Transformation
	12 GP Data for Secondary Uses
D. Integrated Care	13 Integrated Care - Business Change
	14 Integrated Care - Interoperability and Architecture
	15 Social Care Integration

OFFICIAL

	16	Personal Health Record
E. Digital Medicines	17	Digitising Community Pharmacy
	18	Pharmacy Supply Chain and Secondary Uses
	19	Integrating Pharmacy Across Care Settings
F. Elective Care	20	Digital Referrals
G. Paper-free at the Point of Care	21	Driving Digital Maturity
	22	Digital Child Health
	23	Digital Diagnostics
	24	Workforce and Professional Capabilities
H. Data Outcomes for Research and Oversight	25	National Data Services Development
	26	Data Content
	27	Innovative uses of Data
I. Infrastructure	28	Digital Interoperability Platform and Spine
	29	NHSmail2
	30	HSCN
	31	WiFi
J. Public Trust and Security	32	Cyber Security Programme
	33	National Opt-Out Model

Appendix B: Corporate IG Resources



Region IG Lead- summary of roles

- Support the Region in completing NHS England's IG Toolkit assessment, collating evidence, scoring the requirements and liaising with the Corporate IG team for the final NHS England submission.
- Prepare an action/ improvement plan which will require approval by the Region IG group.
- Co-ordinate the Region IG group.
- Attend the National IG Steering Group.
- Ensure the Region contractors / support organisations have adequate IG arrangements in place, supporting procurement exercises to ensure all 3rd parties are compliant with relevant standards.
- Ensure staff complete the mandatory IG training and provide updates to the Region IG group and provide alternative IG training as required.
 - provide advice regarding subject access request
- Undertake compliance audits in accordance with the IG toolkit.
- Develop local sharing agreements as required.
- Provide support/ undertake privacy impact assessments where required for any new processes.
- Ensure fair processing notices are adequate for flows of personal confidential information.
- Maintain the Region section (incorporating localities) of the NHS England information asset register. Assist IAO's with undertaking risk assessments.
- Manage information security incidents, produce lessons learnt, manage and investigate and report SIRI's including reporting to SIRO / deputy SIRO and Corporate IG team.
- Undertake risks management and provide a copy of the risk to Central IG risk and issue register
- Undertake the role of records management co-ordinator for the region/ locality and supports Information Management Audits (records management, data quality and confidentiality audits)

Locality team nominated Senior IG lead

Each locality team has a nominated senior IG lead who has local accountability for IG. They are a point of escalation for local IG issues to the locality SMT. They are members of the region IG group and they provide support to the region IG leads as appropriate.

IG Officers – summary of roles

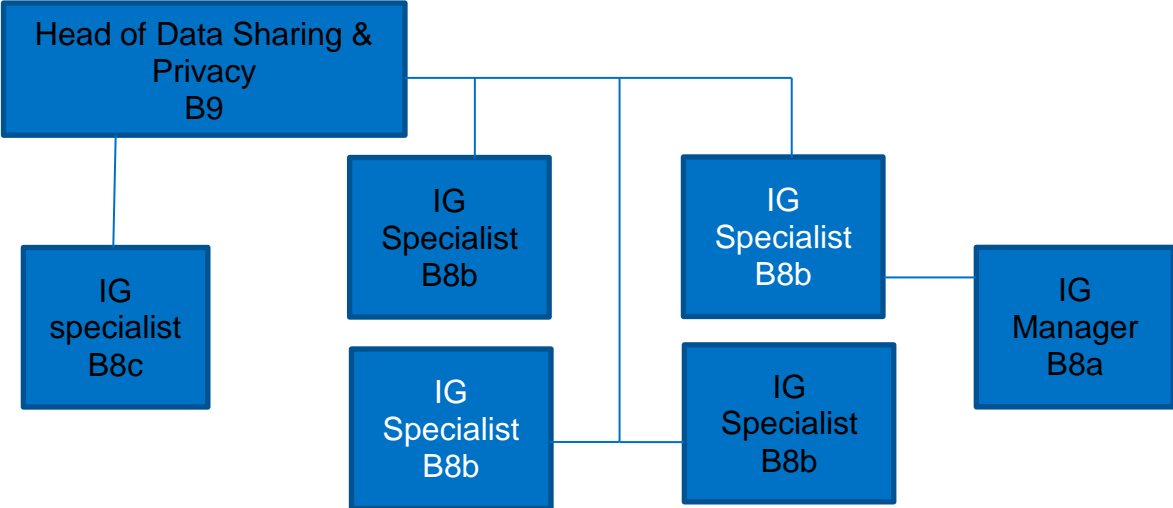
- Support the local teams in collating evidence for the requirements in the IG Toolkit assessment and liaising with the Region IG Lead for the final NHS England submission.
- Support the local teams with the development and delivery of their IG Toolkit action/improvement plans monitor progress and report to the Region IG Group
- Produce reports and present these to the region IG group.
- Ensure the region / local team contractors / support organisations have adequate IG arrangements in place.

OFFICIAL

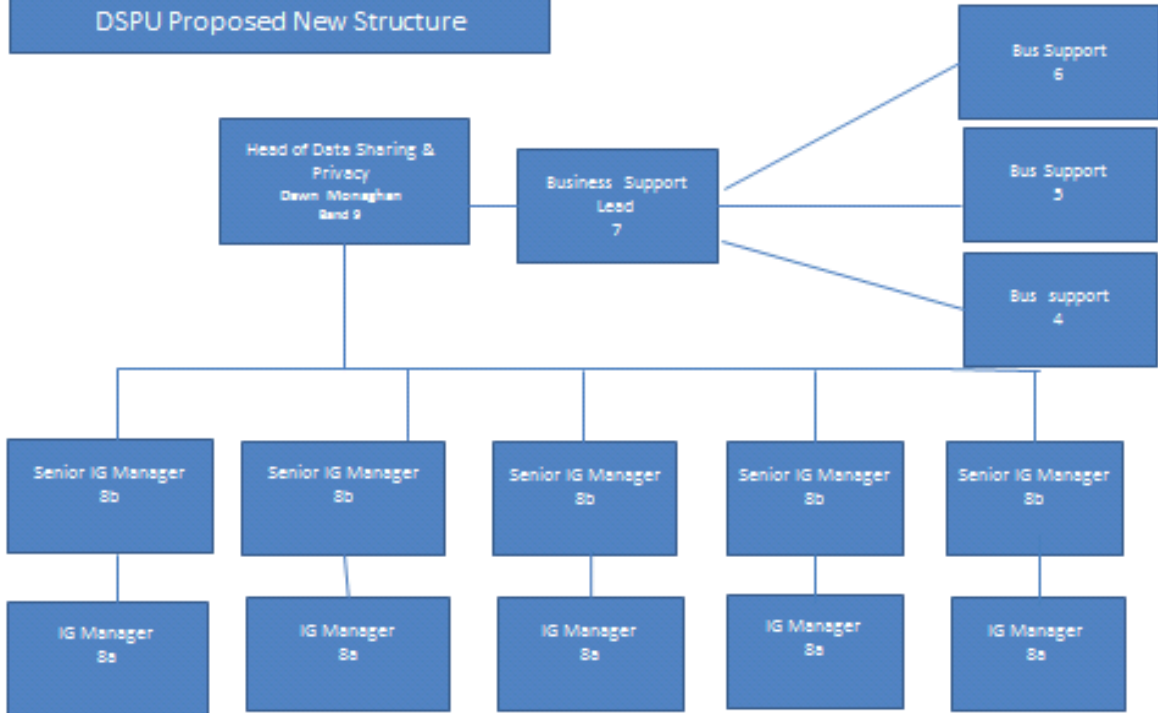
- Ensure staff complete the mandatory IG training and provide updates to the region IG group and work with the Region IG lead to provide alternative IG training as required.
- Develop the local subject access request (SAR) checklist in line with the national SAR procedure
- Undertake compliance audits in accordance with the IG toolkit.
- Support the development of local information sharing agreements as required and undertake work to embed these within sub-regional teams.
- Provide support/undertake privacy impact assessments where required for any new processes.
- Ensure fair processing notices are adequate for flows of personal confidential information.
- Support the Region IG Lead in maintaining the information asset register. Assist IAO's with undertaking risk assessments.
- Support the management and response to information security incidents
- Undertake the role of records management co-ordinator for the region/ local teams and support records management audits.
- Provide IG support to the local teams IG Groups and or SMT meetings.

Appendix C: DSPU Team Structure

DSPU Present Team Structure



DSPU Proposed New Structure



Appendix D: SIRO Responsibility and Assurance for NHS England, CCGs and CSUs

SIRO Responsibility	NHS England SIRO (supported by regional deputy SIROs)	CSU SIRO	CCG SIRO	Comments
<p>1.To be accountable for NHS England’s information risk governance to the Board, supported by the Information Asset Owners</p>	<p>To be accountable to NHS England Board for the management of information risks within the organisation (including CSUs) and for holding Directors and other Information Asset Owners (IAOs) to account for the management of information assets and related risks and issues within their respective remits..</p> <p>To ensure that IG, information and cyber security are dealt with at the highest level of management.</p> <p>To be responsible for oversight of assurance of CSU and CCG IG, information and cyber security- see note 1.</p>	<p>To be accountable to the CSUs accountable officer and NHS England’s SIRO for the management of risks within the CSU and for holding Directors and other Information Asset Owners (IAOs) to account for the management of information assets and related risks and issues within their respective remits.</p> <p>To ensure that IG, information and cyber security are dealt with at the highest level of management.</p> <p>Where a CCG commissions the CSU to provide services that requires them to establish information systems, the CSU is accountable to the procuring commissioner for the information and cyber security controls as part of the data processor agreement.</p>	<p>To be accountable to the CCGs Accountable Officer for the management of information risks within the organisation and for holding Directors and other Information Asset Owners (IAOs) to account for the management of information assets and related risks and issues within their respective remits.</p> <p>To ensure that IG, information and cyber security are dealt with at the highest level of management.</p> <p>Responsible for information held by the CCG including information held by a contracted data processor.</p> <p>Responsible for oversight of assurance of commissioned service provider’s IG and cyber security compliance</p> <p style="text-align: center;">-</p>	<p>Note 1: See operating model activity 5.2.11 for further details of CCG IG Assurance and activity 5.2.12 for further details of CSU IG assurance.</p>

OFFICIAL

		Provide assurance to NHS England regarding CSU IG and Cyber security compliance.		
	<p>To advise the Board on the potential impact of information risks and issues from across the organisation (including CSUs) on NHS England's strategic objectives and policy; operating model.</p> <p>To provide reports to the Board on the performance of NHS Commissioners' and providers' conformance with Information risk management requirements, including an overview of serious incidents and their management.</p> <p>To advise the Board on strategic system-wide issues and their potential solutions and gain their support for work to be undertaken in collaboration with key stakeholders.</p>		<p>To advise the Board/Governing Body on the potential impact of information risks and issues across the organisation and recommend mitigation.</p> <p>To provide reports to the Board on the performance and conformance with Information risk management requirements, including an overview of serious incidents and their management.</p> <p>To advise the Board on strategic system-wide issues and their potential solutions and gain their support for work to be undertaken in collaboration with key stakeholders.</p>	
2.Take overall ownership of the organisation's IG and information risk management framework	To act as the figurehead for IG within the organisation: leads the NHS IG risk assessment and management processes; Oversees compliance with regulatory, statutory and organisational information and	To act as the figurehead for IG within the CSU: leads the NHS IG risk assessment and management processes; Oversees compliance with regulatory, statutory and organisational information and	To act as the figurehead for IG within the CCG: leads the NHS IG risk assessment and management processes; Oversees compliance with regulatory, statutory and organisational information and	Note 2: As part of NHS England's CCG Assurance programme – although IG is not currently included

OFFICIAL

	<p>cyber security policies and standards.</p> <p>To provide advice to the Board on the effectiveness of information risk management across the organisation.</p> <p>Has devolved responsibility to act on behalf of the Board to ensure that IG and Cyber security roles played by NHS England are fulfilled.</p> <p>The SIRO is expected to understand how the strategic business goals of the organisation and how other NHS organisations business goals may be impacted by information and cyber security risks and ensure action is taken to ensure those risks are managed.</p> <p>To take ownership of information risk policy, act as a champion for information risk on the Board.</p>	<p>cyber security policies and standards.</p> <p>To ensure that NHS England's Information risk procedure is adhered to and risks and issues escalated appropriately to the NHS England SIRO.</p>	<p>cyber security policies and standards.</p> <p>Provide assurance to NHS England that information risks are managed appropriately. (See note 2)</p>	<p>in the CCG Assurance Framework</p>
<p>3. To ensure commissioner assurance of IG for directly commissioned services</p>	<p>To ensure that providers of directly commissioned services are held to account for their IG, information and cyber security arrangements. see Note 3</p>		<p>To ensure that providers of directly commissioned services are held to account for their IG, information and cyber security arrangements. see Note 4</p>	<p>Note 3- see operating model activity 5.2.10 for further details regarding assurance for</p>

OFFICIAL

	<p>To provide assurance to the Board that directly commissioned providers are operating to mandated IG and cyber security standards.</p>			<p>primary care and specialised commissioning.</p> <p>Note 4:CCG can contract the CSU to assure commissioned service providers IG performance</p>
<p>4.To be responsible for oversight and assurance for commissioning bodies (e.g. CCGs) for indirectly commissioned services (CCGs)</p>	<p>Responsible for ensuring that CCG s are operating to mandated IG standards and assuring that the providers of the services they commission are likewise operating to mandated IG standards.</p> <p>Responsible for statutory guidance which can include guidance for commissioners, on how they should hold their providers to account and the standards that should be met.</p>		<p>Assuring their commissioned service providers are operating to mandated IG and cyber security standards.</p> <p>CCGs are responsible for driving improvement in standards of IG within their commissioned provider services. Where a CCG contracts with a provider for health care services they must use NHS Standard contract (IG is embedded in clause 21, requiring IGT completion and commission of independent audit to assure the self assessment)</p> <p>Take a lead in providing assurance to NHS England that their commissioned service providers have appropriate data and cyber security controls in place to protect the information they hold.</p>	<p>See operating model activity 5.2.12 for suggested operational procedures for this assurance to be provided by CCGs to NHS England</p>

OFFICIAL

			To ensure contract monitoring is undertaken and providers held to account.	
5. Provide written advice to the Accounting Officer on the content of the organisation's statement of internal control in regard to information risk	To provide written advice to the accounting officer on the content of the organisations statement of internal control in regard to information risk. (this includes CSUs)	To provide information e.g. IG Toolkit compliance, number of security incidents etc to NHS England for inclusion in the organisations statement of internal control.	To provide written advice to the CCG accounting officer on the content of the organisations statement of internal control in regard to information risk	
6. Own the organisation's information incident management framework and support the management of all information assets	To ensure that the organisation has implemented an effective information incident management and response capability that supports the sharing of lessons learned. Provide assurance to the Board that corporate incidents are monitored and investigated appropriately, including CSU incidents. Provide assurance to the Board that CCGs and their providers are reporting, investigating and managing incidents appropriately.	To ensure that NHS England's Incident reporting procedure is adhered to.	To ensure that the organisation has implemented an effective information incident management and response capability that supports the sharing of lessons learned. To ensure that CSU incidents are managed and investigated where the CSU is acting as a data processor for the CCG. Provide assurance to NHS England that CCG incidents are reported, investigated and monitored appropriately and that they are monitoring the incidents of their providers.	
7. Championing effective IG and risk management across	To liaise, as needed, with the internal patient safety team, NHS Digital the CQC to ensure			

OFFICIAL

the system	there is effective monitoring of IG performance and serious incidents reporting across the system.			
	To commission and receive reports from NHS Digital and CQC about IG performance and serious incidents.			
	To liaise with key stakeholders on system wide information risk management issues and to bring these to the attention of the Board, as appropriate.			
	Highlight information risks arising from the NHS in England that impact upon NHS England's strategic objectives and operational delivery.			

Appendix E: Terms of Reference

National IG Steering Group

National IG Steering Group – Terms of Reference



National IG Steering
Group Terms of Refer

Central Team IG Operational Group

Central Team IG Operational Group – Terms of Reference





Terms of Reference -
Central Team IG Gro

Records Management Co-ordinators Group




20160121 RMC
Slides TOR v 2.0 final


Appendix F: Internal IG Assurance and Legal Compliance

Task	Central Team	Region	Local Office
IG Framework- Roles <i>IG Toolkit Ref: 101</i>	Appoint a national SIRO and deputy SIRO for the Central Team Appoint national Caldicott Guardian and deputy for central team.	Appoint deputy SIRO. Appoint local CG, Region IG lead (See appendix B).	Appoint local CG. Nominate Senior IG lead (see Appendix B). Appoint IG officers (see Appendix B for structure chart).
<i>Associated documents:</i>  IG Policy V3.0.docx	Maintain contact details on central SharePoint register, including details of CSU IG leads, SIROs and CGs. See appendix B for organisation chart	Maintain contact details on central SharePoint register.	Maintain contact details on central SharePoint register.
IG Framework – Groups <i>IGT ref: 101</i>	National IG Steering Group (see appendix E). Central Team IG Operational Group (see appendix E). Records Management Co-ordinators (see appendix E).	Region IG operational Group- quarterly or bi-monthly. The Region IG Operational Groups to provide upward reports to the Central Team IG Operational Group on a quarterly basis on operational risks and progression with the IG Toolkit improvement plan.	Local IG group. Provide upward report to the Region IG operational Group.
 IG Policy V3.0.docx	Corporate IG team – monthly meetings. Region IG leads weekly telecons. CSU IG leads meeting.		


OFFICIAL

	Attend medical directors meeting to discuss Caldicott issues.		
IT Security	The Head of Corporate ICT Technology & Security is the IT security officer and is responsible for IT security requirements.		
 Information Security Policy V3.0.pdf			
Cybersecurity	A joint approach with ICT and Business Continuity to ensure that cybersecurity is incorporated into relevant policies and procedures for internal processes. NIB domain J is responsible for cybersecurity requirements for the wider system and support for this is provided by DSPU.		
IG Policies and Procedures	Maintain and develop IG policies and procedures.	Assist with development of IG policies and procedures and review for region alignment.	Disseminate and embed IG policies and procedures in teams.
<i>IG Toolkit Ref: 105</i>	Review all policies on annual basis.		


OFFICIAL

<p>A full list of policies can be found in the IG handbook, page 18</p>	<p>Review IG handbook at team meetings and update where required.</p> <p>Disseminate new/ amended versions appropriately.</p>	<p>Disseminate and embed IG policies and procedures in region.</p>	
<p>IG Training</p>	<p>Develop training needs analysis and approval from CTIGOG.</p>	<p>Monitor specialised training e.g. IAO/CG/RM and store evidence locally for region staff.</p>	<p>Monitor specialised training e.g. IAO/CG/RM and store evidence locally.</p>
<p><i>IG Toolkit Ref: 112</i></p>	<p>Prepare monitoring reports of compliance and distribute to regions (for annual training modules and IG handbook).</p>	<p>Disseminate compliance report to local teams.</p>	<p>Receive compliance reports regarding standard training and target staff that are not compliant.</p>
<p> IG Training Programme 2016-201</p>	<p>Maintain refresher IG module.</p> <p>Raise awareness of the requirement to complete IG training.</p> <p>Escalate any associated risks with IG training.</p>	<p>Provide exception report to central team.</p> <p>Region IG leads to undertake specialised IG training.</p> <p>Raise awareness of the requirement to complete IG training.</p>	<p>IG officers to undertake specialised IG training.</p> <p>Raise awareness of the requirement to complete IG training.</p>


OFFICIAL

<p>IG Toolkit</p>	<p>Develop national action plan, CTIGOG to monitor progress. Collect evidence for CT and store evidence in SharePoint.</p> <p>Report to SIRO on risks.</p> <p>Undertake IGT assessments and submit final assessment.</p>	<p>Region IG leads to contribute to development of national action plan.</p> <p>Undertake actions required at region level from national action plan and store evidence in repository.</p>	<p>IG officers to undertake actions from national IG action plan and store evidence in repository. Report to local IG group on progress and report exceptions to region IG leads. Undertake peer reviews of evidence.</p>
<p> IGT Assurance Process 2016-17.pdf</p>	<p>Develop approval process for submissions. (See approval process for 2015/ 16 assessment embedded document).</p> <p>Provide the Central Team Operational IG Group with progression reports on a bi-monthly basis.</p> <p>Prepare annual report for Board/ Audit committee.</p> <p>Assign 'owners' for IG requirements.</p> <p>Facilitate internal audit assurance.</p>	<p>Region IG leads collate local team exceptions and report to region IG group and central team bi monthly.</p> <p>Region IG leads to quality check evidence provided by local teams.</p> <p>Region IG leads to work collectively to provide assurance on levels prior to submission of assessments.</p>	
<p>Contracts</p>	<p>Maintain contracts register on SharePoint for central team contracts.</p> <p>Review annually, collate region and teams information and present findings to CTIGOG.</p> <p>Update contracts where required.</p>	<p>Maintain contracts register on SharePoint for region contracts.</p> <p>Review annually and inform Central Team IG lead.</p> <p>Update contracts where required.</p>	<p>Maintain contracts register on SharePoint for local team contracts.</p> <p>Review annually and inform Central Team IG lead.</p> <p>Update contracts where required.</p>
<p><i>IG Toolkit Ref: 110</i></p>			
<p>Contracts on IG SharePoint page</p>			


OFFICIAL

<p>Information Sharing Agreements</p>	<p>Maintain information sharing agreements register on SharePoint for central team.</p>	<p>Maintain information sharing agreements register on SharePoint for region.</p>	<p>Maintain information sharing agreements register on SharePoint for local teams.</p>
<p><i>IG Toolkit ref: 207</i></p>	<p>Review annually, collate region and teams information and present findings to CTIGOG.</p>	<p>Review annually and inform Central Team IG lead.</p>	<p>Review annually and inform Central Team IG lead.</p>
<p>Information Sharing Agreement register</p>	<p>Update information sharing agreements where required.</p>	<p>Update information sharing agreements where required.</p>	<p>Update information sharing agreements where require.</p>
<p>Compliance Audits</p>	<p>Develop framework template, undertake audits in Quarry House and Skipton House. Report findings to the CTIGOG.</p>	<p>Develop audit schedule for region and undertake audits. Report findings to region IG group.</p>	<p>Develop audit schedule for local teams and undertake audits. Report findings to region IG group.</p>
<p><i>IG Toolkit ref: 206, 440, 604</i></p>			
<p> Information Management Audit Fr</p>	<p>Implement any remedial actions.</p>	<p>Implement any remedial actions</p>	<p>Implement any remedial actions.</p>
<p>IG Compliance Questionnaire</p>	<p>Develop and maintain IG Spot check/ service questionnaire to monitor IG awareness across the organisation.</p>	<p>Disseminate findings and implement remedial actions as required.</p>	<p>Disseminate findings and implement remedial actions as required.</p>
<p><i>IG Toolkit ref : 111,112,201,601,603</i></p>	<p>Conduct annually, communicating to staff via Engage. Present findings to CTIGOG.</p>		


OFFICIAL

	<p>IG Induction Questionnaire-monitor the effectiveness of induction process in promoting IG awareness across organisation.</p> <p>Present report to CTIGOG.</p>		
Information Asset Management	<p>Allocate IAOs and IAAs for all CT information assets and ensure that they undertake relevant training.</p>	<p>Allocate IAOs and IAAs for all region information assets and ensure that they undertake relevant training.</p>	<p>Allocate IAOs and IAAs for all local team information assets and ensure that they undertake relevant training.</p>
<p><i>IG Toolkit ref: 202,207,301,305,307,308, 309,310,311,313,323</i></p>	<p>Coordinate and maintain Central Team/Directorate information asset register with associated information flows, risks and action plans.</p>	<p>Coordinate and maintain Region information asset register with associated information flows, risks and action plans.</p>	<p>Coordinate and maintain local team information asset register with associated information flows, risks and action plans.</p>
<p> Information Asset Management Procedu</p>	<p>Provide reports on a quarterly basis to deputy SIRO.</p> <p>Ensure that the information on the asset register adheres to the agreed standards and highlight any risks.</p> <p>Maintain the list of processing occurring outside of the UK</p>	<p>Provide reports on a quarterly basis to region deputy SIRO.</p> <p>Ensure that the information on the asset register adheres to the agreed standards and highlight any risks.</p>	<p>Provide reports on a quarterly basis to region deputy SIRO.</p> <p>Ensure that the information on the asset register adheres to the agreed standards and highlight any risks.</p>
New Processes, Services and Systems	<p>Working with business teams, provide advice and guidance for national systems and processes.</p>	<p>Working with business teams provide advice and guidance for region and local team systems and processes.</p>	<p>Working with business teams, provide advice and guidance for region and local team systems and processes. (See flowchart of pia and risk assessment approval</p>
<p>IGT ref: 210</p>	<p>Develop SLSP in compliance with</p>	<p>(See flowchart of pia and risk</p>	


OFFICIAL

<p>(Awaiting revised procedure to embed document)</p>	<p>template in the IG procedure.</p> <p>Ensure IAOs/ IAAs are allocated and the IAM updated accordingly.</p> <p>Finance/ procurement, ICT, PMO to alert IG to any new projects that may require IG consideration.</p>	<p>assessment approval process in the embedded procedure).</p> <p>Develop SLSP in compliance with template in the new processes procedure.</p> <p>Ensure IAOs/ IAAs are allocated and the IAM updated accordingly.</p>	<p>process in the embedded procedure).</p> <p>Develop SLSP in compliance with template in the new processes procedure.</p> <p>Ensure IAOs/ IAAs are allocated and the IAM updated accordingly.</p>
<p>Privacy Impact Assessments</p>	<p>Develop the PIA template and approval process.</p>	<p>Provide support to the region and locality business areas that are considering new processing of personal data with the completion of the PIA.</p>	
<p> 20160620 PIA-DPA-DSA Approv</p>	<p>Provide support to the business areas that are considering new processing of personal data with the completion of the PIA.</p> <p>Ensure IAOs/ IAAs are allocated and the IAM updated accordingly.</p> <p>Ensure the relevant deputy CG / deputy SIRO and / or CG / SIRO approval is obtained.</p> <p>Maintain the central register for approved PIA's.</p>	<p>Ensure IAOs/ IAAs are allocated and the IAM updated accordingly.</p> <p>Ensure the relevant deputy CG / deputy SIRO and / or CG / SIRO approval is obtained.</p> <p>Maintain the central register for approved PIA's.</p>	
<p>Caldicott Issues Log</p>	<p>Develop national log on SharePoint.</p>	<p>Maintain Caldicott issues log for region (on central SharePoint) and discuss</p>	<p>Maintain Caldicott issues log for local teams (on central SharePoint).</p>
<p><i>IGT ref: 200</i></p>	<p>Maintain log for central team issues. Review the national log on a quarterly</p>	<p>region and local team issues at</p>	


OFFICIAL

<p>Caldicott Issue log</p>	<p>basis for consistency and report to CT IGOG.</p> <p>Medical directorate to inform Corporate IG of any requests received directly.</p>	<p>region IG group.</p> <p>Review of the log for consistency across the region.</p>	
<p>DPA- Notification</p> <p><i>IGT ref: 209</i></p>	<p>Maintain DPA Notification, Undertake annual check for purposes, oversees processing etc.</p>	<p>Inform the CT IG team of any processing of PCD occurring outside of the UK, check for purposes not included on the notification.</p>	<p>Inform the CT IG team of any processing of PCD occurring outside of the UK.</p>
<p>DPA- Subject Access Requests</p> <p><i>IGT ref: 205</i></p> <p> Subject Access Request Procedure v.</p>	<p>Develop & maintain Subject Access Request procedure.</p> <p>Ensure staff dealing with SAR's are appropriately trained, Manage CT SAR's requests.</p> <p>Collate SARs figures from region, PCSS and CSUs & CT and present to CTIGOG.</p> <p>Identification of performance and implementation of remedial actions.</p>	<p>Ensure staff dealing with SAR's are appropriately trained, manage regional SAR requests, collate and report SAR compliance figures to the regional IG group.</p> <p>Identification of performance and implementation of remedial actions.</p>	<p>Ensure staff dealing with SAR's are appropriately trained, Manage SAR requests, report SAR compliance figures to the region IG group.</p> <p>Identification of performance and implementation of remedial actions.</p>
<p>DPA- Fair Processing Notice</p> <p><i>IGT ref: 250</i></p>	<p>Maintain fair processing notice for public and staff.</p>	<p>Advise of new fair processing requirements to the business for non- programmes areas.</p>	



OFFICIAL

Data Processing Agreements	Assist with development of data processing agreements for national systems.	Assist with development of data processing agreements for region and local systems.	Assist with development of agreements.
<i>IGT ref:</i>			
 20160620 PIA-DPA-DSA Approv	See embedded flowchart for relevant authorisation process. Maintain list of agreements on central SharePoint register.	See embedded flowchart for relevant authorisation process. Maintain list of agreements on central SharePoint register.	
ICO Investigations	Maintain central log on SharePoint and forward requests to region IG leads as appropriate to investigate and respond.	To investigate, manage and respond to relevant requests. Copy CT IG lead to upload information to the central log on SharePoint.	Support the region IG lead in providing the response to the ICO.
	Investigate and respond to CT requests.		
FOI/ Parliamentary Questions	Assist with responses to requests relating to corporate information.		
	The FOI team to supply compliance reports on a quarterly basis for the CTIGOG.		


OFFICIAL

<p>Incident Management</p>	<p>Monitor incidents received through the incident reporting tool, investigate central team incidents, update incident log, allocate incidents to be investigated to the relevant region IG lead or IG officer.</p>	<p>Investigate region incidents, update IG incident log system via SharePoint. Escalate SIRIs to deputy SIRO and Head of Corporate IG.</p>	<p>Investigate local incidents, update IG incident log system via SharePoint. Escalate any SIRIs to region deputy SIRO and region IG lead.</p>
<p><i>IGT ref: 302</i></p>			
<p> Information Security Incident Reporting Pr</p>	<p>Escalate SIRI to central team deputy SIRO/ national SIRO.</p> <p>Monitor investigation progression and implementation of the action plan to closure.</p> <p>Collate the quarterly incident reports for the CTIGOG, produce regular lessons learned bulletins. Produce quarterly SIRI status reports for the NIGSG.</p> <p>See security incident reporting procedure for flowcharts of reporting processes.</p>	<p>Collate region and local team incident reports for the region IG group.</p> <p>Disseminate lessons learned.</p>	<p>Disseminate lessons learned.</p>
<p>Risks and Issues</p>	<p>The Corporate IG team request the Risk Leads across the Directorate and Regional programme teams to forward a copy of any current IG risks on the local risk register on a bi-monthly</p>	<p>Log all risks and issues on the central IG risk register (SharePoint). Report the risks to the region IG group, escalate any</p>	<p>Log all risks and issues on local risk register. Inform the region IG lead of any IG risks/ issues.</p>
<p><i>Toolkit Ref: 301</i></p>			<p>Amber/red risks escalated to local</p>

OFFICIAL

<p><i>Associated documents:</i></p>  <p>IG risk and issue management procedu</p>	<p>basis.</p> <p>IG risks are collated onto one central IG risk register and these are divided into operational and strategic risks.</p> <p>The top five operational risks are discussed at the Central Team IG operational group and an upward report is presented to the NIGSG.</p> <p>The top 5 strategic risks are determined prior to the NIGSG and these are then reviewed in more detail.</p>	<p>amber/red risks to the deputy SIRO and national SIRO as per NHS's England Risk Management Policy and Guide.</p>	<p>SMT group meeting as per NHS England's Risk Management Policy and guide.</p>
<p>Data Quality</p>	<p>Maintain Data Quality strategy.</p>	<p>Develop local Data Quality plans and undertake audits.</p>	<p>Develop local Data Quality plans and undertake audits. Report findings to the region IG group.</p>
<p><i>IGT ref: 440</i></p>	<p>Develop and maintain data quality plan for CT and undertake regular audits.</p>	<p>Report findings to the region IG group.</p>	
 <p>Data Quality Strategy 1.1.pdf</p>			
<p>Registration Authority</p>	<p>Develop and maintain RA policy.</p>		
<p><i>IGT ref: 303 and 304</i></p>			

OFFICIAL

 <p>Registration Authority Policy 1.0.p</p>			
<p>Business Continuity Management</p>	<p>Liaise with BCP team to ensure that IGT requirements are met and evidenced.</p>		
<p><i>IGT ref: 309</i></p>			
<p>Records Management</p>	<p>Develop and maintain NHS England Document and Records Management Policy</p> <p>Develop and maintain NHS England Retention and Disposal Schedule and Guidance</p> <p>Provide guidance and support to NHS England staff on all aspects of records management</p>		
<p><i>IGT ref: 601 & 604</i></p>			
<p>Annual Report</p>	<p>Write the IG section of the annual report.</p>		

Appendix G: Corporate IG Team Objectives 2016-17

Objective	Lead	Timescale	
Fair Processing Notice	MG	Mar 2017	<p>Finalise PID and project plan by dec 2016</p> <p>Identify and engage with relevant stakeholders by dec 2016</p> <p>Use existing information resources to inform the project e.g. IAMs identifies all information assets that process personal data.</p> <p>Establish project group by dec 2016</p> <p>Draft and report findings to relevant committees/groups.</p> <p>Develop revised notice.</p>
RA Policy	MG	Sep 2016	<p>Work with Head of Workforce Systems and Records Manager to review and update NHS England's RA Policy. Ensure that the policy meets national guidance (NHS Digital RA guidance) and standards (ie requirements 303 and 304 of the IG Toolkit).</p> <p>Work with RA Manager and other key stakeholders to ensure that RA arrangements and processes are fit for purpose.</p> <p>Confirm locality RA arrangements.</p>
HR Data Flows	MG	Oct 2016	<p>Establish working group to review existing arrangements ie what staff data is held, where does it flow from/to, who is it shared with and why.</p> <p>Report on findings and recommendations to Head of IG and Head of Workforce Systems.</p> <p>Develop and agree an action plan to address any remedial actions that are identified.</p> <p>Report on progress to relevant groups/committees.</p>
Overseas Processing Procedure	NL	Sep 2016	<p>Development of an NHS England offshoring policy , ensure it conforms to the HMG offshoring policy.</p>
Off Payroll	AB	Feb 2017	<p>Identify Current year off-payroll workers for the purpose of training and workers contract assurance</p> <p>Assist the central commercial team in developing a process to have off-payroll workers routinely identified, trained (for IG) and appropriate contract signed by end of 16-17 with a view to a pilot roll out and review of effectiveness</p> <p>Assist the central commercial team in developing a process to be piloted with certain employer agencies used</p>

OFFICIAL

			by NHS England for the use of identification of off-payroll workers and pre employment checks, appropriate contracts and pre-employment IG materials and training being given to off-payroll workers before starting their role, by the end of 16-17
IGTT Monitoring Process	NL	Oct 2016	Streamline the process of monitoring IG training across the Central team and regions. Dissemination of relevant staff reporting data to the relevant region / locality
New Processes Procedure	AB	Sep 2016	To scope the most effective ways to implement the new process procedure and PIAs throughout the organisation. Stakeholder engagement with relevant teams/directorates to discuss best approach. Implementation of procedure and review effectiveness.
Guidance for Disclosure of Information (PCSE) and Training	AB	Oct 2016	To conduct a programme of review and improvement on the guidance documents and training given to relevant PCSE staff dealing with information disclosure of GP records. To monitor and review PCSE's administration of information requests for appropriate compliance.
GDPR	AB	Dec 2016	Review impact of new DPA EU directive. To review and report on the differences in GDPR and current DPA in current NHS England BAU functions. To scope how the differences will impact on the operational behaviour of NHS England's current functions. Carry out relevant engagement with teams/functions that will be affected by the GDPR and report on 'gap' in current working practice to GDPR compliant working practice, and how best to change current processes. To scope and report how future projects/ procurements will need to be GDPR compliant compared to current project/ procurements implementation workings. To produce relevant internal guidance documents on GDPR for NHS England staff use.
Health & Justice	PM/ DS	Dec 2016	Scoping exercise being undertaken- more details to follow.
Business as Usual Handover Process	DS	Dec 2016	To develop a handover process for strategic programmes that transfer to corporate Ig as Business as usual.
Policy Management System	DS	Mar 2017	Procure and implement new Policy management system.

OFFICIAL

Complaints Process	TP	Aug 2016	Meet with locality complaints team, propose national solution, submit proposal for sign off. Standardise consent form. Ensure consent complies with DPA, CG 3 and common law of confidentiality Delayed as new complaints process came out and needs impact assessment in addition CG3 needs impact assessment
Spec Commissioning IG Compliance	TP	Oct 2016	Engagement and awareness workshop, agreed time schedule of task compliance, report for other regions of identified issues and proposed solutions Data flows assessment, provider contract impact assessment, SAR impact assessment
IAM Phase 2	TP all	Oct 2016 bau	Awareness workshop, record WebEx to use as training material – this has been done but needs reviewing to ensure completeness IAO/IAA workshop – in progress IAM workshop closure Ensure all risk statuses for assets and data flows are reviewed, revised where necessary in conjunction with the IAAs/IAOs and any risks that are identified are added to the system. Ensure any new IAOs/IAAs have completed mandatory Information Risk training. Establish regular reports on progress/risks/issues to Region IG Group and dSIRO. Ensure that, where unacceptable levels of risk are identified, remedial actions are taken to mitigate the risks to an acceptable level.
Legacy Records	SG	Dec 2016	Proposal is to catalogue legacy records and reduce storage costs. Version 14.0 of legacy paper with Steve Verdon for comment and a view to be taken by Karen Wheeler as to how to proceed. Issue with data quality – some 80,000 boxes have insufficient detail against them in terms of content.
Records Management-closure of primary care contractors	SG	Sep 2016	Process for records management arrangements for closure of primary care contractors.
ERMS	SG	Mar 2017	Launched August 2016. Period of 6 months at least required for the system to begin to be used regularly as a ‘business as usual’ process for staff. Training will be required for all NHS England staff on the system.

OFFICIAL

			Monitoring and assessment of the system required to ensure that records are being uploaded successfully and identify gaps.
Paper Light Challenge	SG	May 2018	Aim is to have a reduction of printing by 50% by May 2018, which will make cost savings of around £400,000 per annum. Quarterly communications to all staff re 'Reduce Your Printing' days. Specific areas to conduct intensive programmes of reduction. Linking with the IT department to provide training for staff in alternatives to printing – such as using SharePoint, OneNote, etc...
Records Management – development of records inventory	SG	Nov 2016	Scoping exercise to be undertaken- more details to follow.
NDG Review:	CM	Dec 2016	Review and implement actions from National Data Guardian Review
PCSE: SAR /AHRA	CM	Sep 2016	Establish legal position regarding responsibilities for access to living and deceased records and provide guidance, review of feasibility for electronic deceased records
IG Operating Model	CM	Oct 2016	Implement and embed the IG Operating Model, including development of assurance model incorporating the SIRO assurance model for IG/data and Cyber security, including : CSU CCG Central
tNR	WH	Mar 2017	The provision of guidance/advice and drafting of agreements for data required by NHS England as commissioner of services and stored/processed on our behalf in the National Repository
CAG	WH	Mar 2017	Provision of support to the DsFC programme in relation to requests for support from the HRA Confidentiality Advisory Group (CAG) for data required for Commissioning, Risk Stratification and Invoice Validation. This also includes ensuring that all organisations undertaking risk stratification/invoice validation provide assurance that their processes are in line with the CAG approvals and that audits are undertaken to verify they meet the conditions. This also includes working with data processor organisations where required to ensure they meet relevant CAG approval conditions.
Anonymised in	WH	On-going	Working with the NHS Digital agree a level of anonymisation of data required by commissioners which ensures

OFFICIAL

line with the ICO code of practice			that it meets the ICO's Anonymisation Code of Practice whilst ensuring it continues to enable them to meet their statutory duties.
Re-ID	WH	On-going	Working with the NHS Digital commissioners to define requirements for a re-identification service which will allow anonymised data to be re-identified when supported by a separate legal basis, i.e. for direct care purposes/safeguarding
NHAIS	WH	On-going	Ongoing management of NHAIS data processing which is undertaken by the NHS Digital. Set up of NHAIS Authorisation Board (NAB) which deals with requests for data extracts/org links required to support direct care or ensure requesting organisation can meet their statutory duties. Provide IG expertise for the transition to PDS
Fire and Rescue:	WH/ JK	On-going	Support NHS England teams to work with the Fire and Rescue Service in line with integrated working arrangements
IGT	ALL	Jul 2016	Develop IG toolkit improvement plan to maintain satisfactory level of compliance and improve requirements where possible
Invoice Validation	MG	On-going	Monitoring of breaches by providers. Reporting on compliance with the IV process