

INFORMATION GOVERNANCE OPERATING MODEL

2020 - 2022

**Corporate Information Governance, NHS England and NHS Improvement
Information Governance Policy Team, NHSX**

NHS England and NHS Improvement



Enabling a lawful and ethical culture for the use of information
to deliver and improve our high-quality patient care

Contents

1. Executive summary	3
2. Introduction	4
3. IG responsibility scope	5
4. Joint working	10
5. Corporate IG team	11
6. IG Policy team (NHSX)	19
7. Governance framework	22
Appendix A – Corporate IG structure	24
Appendix B – IG Policy team structure	28
Appendix C – IG accountability and responsibilities	29
Appendix D – Policies and procedures	31
Appendix E – Legal and NHS mandated frameworks	33
Appendix F – SIRO roles and responsibilities	36
Appendix G – Caldicott Guardian roles and responsibilities	39

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, NHS Improvement and NHSX. It is intended to provide clarity regarding the roles and responsibilities of both the Corporate IG team and the NHSX IG Policy team.

The document describes:

- The overarching IG framework,
- The scope of responsibilities for IG within the organisations
- The IG workstreams and roles, including roles and responsibilities for SIROs, Caldicott Guardians and their deputies
- The activities of the Corporate IG team and how the IG service is delivered
- The programmes of the IG Policy team in NHSX
- The key stakeholders for IG activities
- The assurance processes for NHS England's commissioning activities

The operating model can be used by NHS England, NHS Improvement and NHSX 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 and projects, for example, by undertaking a data protection impact assessment.

2. Introduction

There are 2 teams in NHS England/ NHS Improvement with responsibilities for IG:

- The **Corporate IG team** which sits in the Commercial Directorate and is internally focused on NHS England and NHS Improvement's own internal compliance.
- The **IG Policy team** is part of the Data Policy and Strategy Directorate in NHSX. The IG Policy team develops IG policy for NHSX, NHS England and NHS Improvement and Department of Health and Social Care programmes of work. It is responsible for coordinating the provision of strategic IG guidance and advice to the wider health and care system.

2.1 Corporate IG team

The Corporate IG team within the Commercial Directorate provides a high quality and efficient Information Governance (IG) service across NHS England and NHS Improvement. The team is responsible for internal IG arrangements and records management. These include policies and procedures, information sharing agreements, management of security incidents, IG training, the Data Security and Protection toolkit, information security and data protection compliance, support to the Caldicott Guardian and Senior Information Risk Owner (SIRO).

Details of the team's responsibilities can be found at section 5 and the team structure chart is shown at Appendix A.

2.2 IG Policy team

NHSX is a virtual organisation (not a legal entity) comprising staff from NHS England, NHS improvement and the Department of Health and Social Care (DHSC).

NHSX leads and facilitates the production of system-wide advice and guidance through the Health and Care Information Governance panel. One of its main aims is to enable IG professionals, front line staff and the public to understand the legal obligations and application of the rules.

The NHSX IG Policy team also has a responsibility to aid understanding, ensure consistency and reduce burden through ensuring the simplification of IG by considering and suggesting changes to legislation, approach and ways of working.

Details of the team's responsibilities can be found at section 6 and the team structure chart is shown at Appendix B.

3. IG responsibility scope

As the new organisation works across the health and care system, boundaries can become blurred, as regions become more integrated in the development of Integrated Care Systems (ICSs). The following therefore describes the areas that are in or out of scope to help NHS England and NHS Improvement staff determine whether IG advice and guidance is the responsibility of:

- The Corporate IG team (including Senior Information Risk Owners (SIROs) and Caldicott Guardians (CGs))
- The IG Policy team in NHSX
- Neither of the above

Further details of the accountability and responsibilities of NHS England and NHS Improvement can be found at Appendix C.

3.1 Scope of Corporate IG responsibilities

3.1.1 NHS England and NHS Improvement responsibilities

As public authorities, both NHS England and NHS Improvement (made up of the NHS Trust Development Authority and Monitor) are a controller under data protection legislation for their activities that require the processing of personal data.

The organisations act as sole controllers for some purposes and may act as a joint controller for others, either with each other or with other organisations, such as the collection of screening data that is undertaken jointly between Public Health England and NHS England.

In its role as a controller NHS England and NHS Improvement must assure any contracts and agreements with its data processors (any suppliers who process personal data on our behalf). The obligations of a data processor were strengthened under the General Data Protection Regulation (GDPR). Whilst data processors may still only act under instruction from a controller, if the data processor fails to meet any requirement of the new legislation that applies to them then they may be liable to claims from data subjects, regulatory action by the Information Commissioner's Office (ICO), or action for breach of contract by NHS England or NHS Improvement. Controllers also have an increased responsibility to secure guarantees that data processors are GDPR compliant before entering into contracts with them. NHS England and NHS Improvement have established robust templates and processes to seek this assurance.

In specific and limited circumstances, NHS England and NHS Improvement may act as a processor under instructions from another controller organisation. In such cases, NHS England and NHS Improvement will enter into a data processing agreement with the controller and work under their explicit instructions.

3.1.2 Directly commissioned services

NHS England directly commissions services such as armed forces, health and justice, specialised commissioning, dentists, pharmacists and opticians.

Commissioning contracts with providers contain either specific requirements to comply with IG requirements, or more general requirements to comply with legislation which will include GDPR.

IG assurance is provided during procurements and contract monitoring and this is supported by the Corporate IG team. **NHS England is not responsible for assuring itself that providers of directly commissioned services are GDPR compliant; see 3.3.1 below.**

Any major incident within these providers that is likely to have a reputational impact or require policy or systems advice would fall to the IG Policy team in NHSX (see 3.2 Scope of IG Policy team responsibilities).

3.1.3 Commissioning Support Units (CSUs)

Commissioning Support Units (CSUs) are not legal entities and are hosted by NHS England, therefore they cannot be a controller or processor in their own right. In the case where CSUs are processing data for their own purposes, NHS England is the controller. Where a CSU is processing data on behalf of a Clinical Commissioning Group (CCG), or other contracted entity, they act as a data processor and NHS England is responsible for this action for example, if the ICO issued a fine to a CSU or enforcement notice then this would be served against NHS England.

3.2 Scope of IG Policy team responsibilities

3.2.1 Responsibilities to health and social care organisations

The Health and Social Care Act 2012 (s.13S) places an obligation on NHS England to publish guidance for registered persons on the practice to be followed by them in relation to the processing of:

- Patient information
- Other information obtained or generated in the course of the provision of the health service.

Registered persons must have regard to that guidance. A registered person is defined by the Health and Social Care Act 2008 as those organisations that are regulated by the Care Quality Commission (CQC). This includes ambulance services, care homes, children's services, clinics, community services, dentists, GPs, hospices, hospitals, mental health services, secure settings and home care agencies.

The NHSX IG Policy team are tasked with ensuring the above functions are met. They have a responsibility to provide advice and guidance to the wider Health and Care system. They provide advice regarding any major IG incident impacting upon the system which may have a reputational impact or require policy or systems advice.

3.3 Out of scope

3.3.1 Registered providers and commissioned services

NHS England, NHS Improvement and NHSX do not have any responsibility for assurance that registered providers or directly commissioned services are GDPR compliant.

- It is the providers themselves who have a legal obligation, as a controller, to meet their legal obligations.
- It is the CQC that is legally tasked with monitoring the IG practices of those they regulate (registered providers) and the ICO's remit to investigate and enforce should a breach notification or complaint require them to take action. The CQC must also keep both NHS England and NHS Improvement informed about the practice followed by registered providers in relation to the processing of personal data.
- Commissioning contracts with providers contain either specific requirements to comply with IG requirements, or more general requirements to comply with legislation which will include GDPR. NHS England will therefore have the means to address any significant failings with providers by means of contractual action if it considers this appropriate in any particular case. The NHS Standard and Primary Care Contracts are being strengthened to explicitly reference GDPR requirements as part of a compliance programme.

3.3.2 Secondary care

Foundation Trusts, NHS Trusts and independent secondary care providers are legal entities and therefore controllers in their own right. There is no obligation on NHS England, NHS Improvement or NHSX to obtain assurance from these organisations that they are compliant with the requirements of the GDPR.

3.3.3 Clinical Commissioning Groups (CCGs)

Clinical Commissioning Groups (CCGs) are legal entities and therefore controllers in their own right. There is no obligation on NHS England, NHS Improvement or NHSX to obtain assurance from CCGs that they are compliant with the requirements of the GDPR.

Retrospectively, NHS England is required to conduct a performance assessment of each CCG for each financial year, assessing how well it has discharged its functions. This is completed through the CCG Improvement and Assessment Framework (CCG IAF) managed by the NHS England Assessment Team. The processing of patient information by a CCG is ancillary to its general function of securing the provision of health services and therefore IG does not need to be a core component of a performance assessment. However, if there have been significant IG breaches on the part of a CCG, this may represent a general failing to discharge its functions well which would be relevant to NHS England's performance assessment. A significant IG breach by a CCG could also warrant use of NHS England's powers of intervention.

It would therefore be appropriate to make limited enquiries about IG, such as whether the CCG has had any monetary penalties imposed by the ICO or any complaints upheld by the ICO, as part of its performance assessment. NHSX will arrange monitoring arrangements with the ICO.

3.4 Cyber security

The NHS England and NHS Improvement Information and Cyber Security team has the responsibility of maintaining security and providing assurance for all internal devices, networks and systems of NHS England, NHS Improvement, NHSX, and those bodies for whom we provide infrastructure.

Being the subject matter experts, the team provides guidance to all staff on matters pertaining to information security best practice, secure and safe architecture of new digital services and applications, due diligence and background checks for new suppliers and solutions, support with information security documentation and fulfilment of any regulatory or statutory requirements pertaining to information and cyber security.

The team works closely with colleagues in the IT and Corporate IG teams to provide guidance, assurance and support on all matters related to its subject matter. With support from these teams they carry out assurance audits and assessments of various systems and applications within NHS England and NHS Improvement for things like access control, vulnerability management, information asset documentation, the review of system level security policies and support for DPIAs.

The team carries out technical investigations into any machines or network devices which may present evidence of malicious code or unauthorised access. They run security assessments and penetration tests on all of NHS England and NHS Improvement’s internet facing websites and applications to ensure they are patched, up to date and do not have any vulnerabilities which can be exploited by malicious actions.

The team also works closely with the NHSX Virtual Chief Information Security Officer (CISO) function for assurance.

Currently the team does not have responsibility for other healthcare bodies. That responsibility falls within the realm of NHSX and NHS Digital. Work is ongoing to define scope so this may change in the future.

3.5 Summary of IG responsibilities

	Corporate IG team responsibilities	IG Policy team responsibilities
NHSE and NHSI teams	<ul style="list-style-type: none"> • IG advice and guidance, where NHS England and NHS Improvement are controllers or processors, including: <ul style="list-style-type: none"> - IG incident management - IG risk and issue management - Data Protection Impact Assessments - Data processor assurance - Subjects’ rights requests - Record of processing - Data sharing - Data governance controls - Information asset management - Records management 	<ul style="list-style-type: none"> • IG advice to NHSX programmes and teams, such as AI / social care <p><i>Note that this area of support is currently under review within NHSX and may change</i></p>

	Corporate IG team responsibilities	IG Policy team responsibilities
Directly commissioned services e.g. GPs, dentists, opticians, specialised commissioning providers	<ul style="list-style-type: none"> • Contract monitoring advice • Procurement advice 	<ul style="list-style-type: none"> • Advice regarding any major incident within these providers that is likely to have a reputational impact or require policy or systems advice • Publish guidance for registered persons on the practice to be followed by them in relation to the processing of: <ul style="list-style-type: none"> - Patient information - Other information obtained or generated in the course of the provision of the health service
CSUs	<ul style="list-style-type: none"> • IG assurance: <ul style="list-style-type: none"> - Ensure adherence to the Deputy DPO Risk Escalation framework, subjects' rights requests, IG incidents, DPIAs, IG risks and issues, record of processing activities - DPO support for high risk processing activities 	<ul style="list-style-type: none"> • None
CCGs	<ul style="list-style-type: none"> • None 	<ul style="list-style-type: none"> • A significant IG breach by a CCG could warrant use of NHS England's powers of intervention. NHSX will establish monitoring arrangements with the ICO
NHS Trusts	<ul style="list-style-type: none"> • None 	<ul style="list-style-type: none"> • Advice regarding any major incident within these providers that is likely to have a reputational impact or require policy or systems advice
Cyber security	<ul style="list-style-type: none"> • Provide input and support where relevant to the Information and Cyber Security team (part of Corporate ICT and Smarter Working), which is responsible for providing guidance for internal NHS England and NHS Improvement staff 	<ul style="list-style-type: none"> • Consult the NHSX Cyber Security team before publishing any guidance relevant or connected to information or cyber security

Fig 1: Summary of IG responsibilities

4. Joint working

NHS England and NHS Improvement (comprising the Trust Development Authority and Monitor) are cooperating to establish a joint enterprise. This mirrors the focus of the NHS Long Term Plan on how we deliver integrated care to patients at a local level, how they set the whole of the NHS up to do that and how it will benefit patients and communities.

To make sure that we comply with our data protection obligations NHS England and NHS Improvement have entered into a [Joint Controller and Information Sharing Framework Agreement](#) which sets out their data protection responsibilities when processing personal data for NHSX's purposes.

The purpose of this agreement is to set out the responsibilities of the Parties when they are acting as joint data controllers or sharing personal data as individual controllers. Setting out these responsibilities and making arrangements that put them into effect assists the Parties to understand their respective responsibilities and the actions they need to take to comply with data protection law. This supports them in achieving their duties to cooperate and helps to deliver the seamless integration of the exercise of their functions.

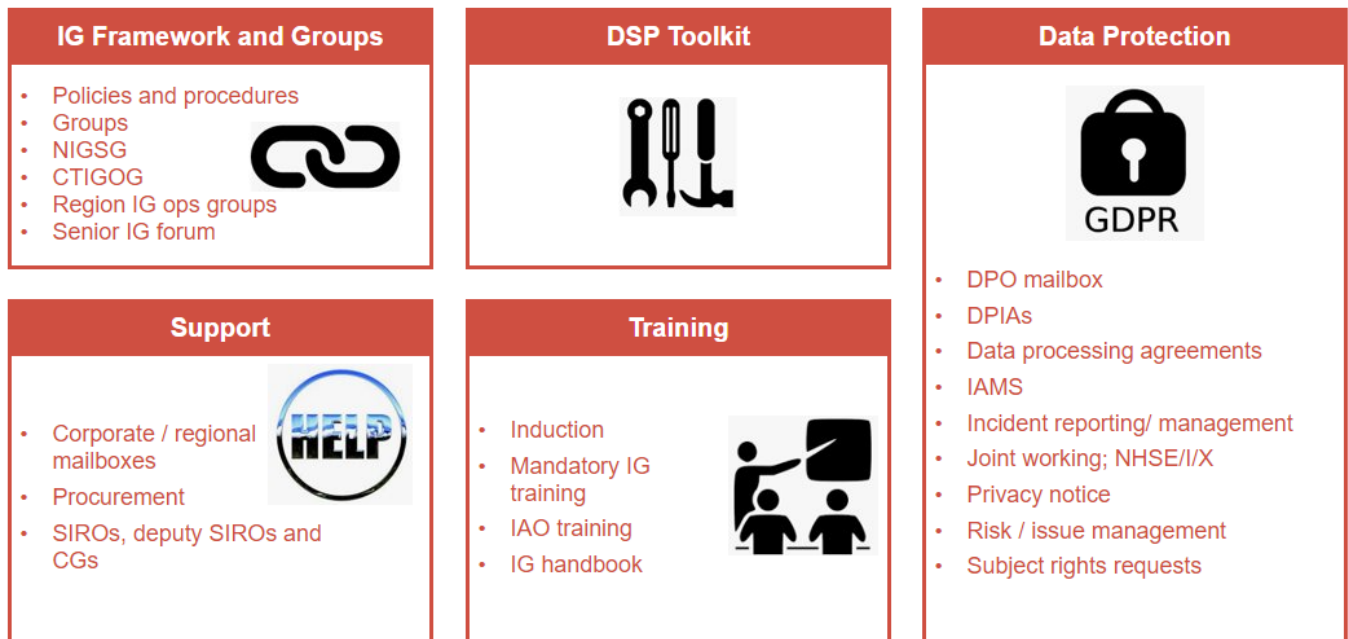
NHS England and NHS Improvement are parties to NHSX, with the Department of Health and Social Care for the Secretary of State. The purpose of NHSX is to take forward digital transformation in the NHS, allowing patients and staff to benefit from the latest digital systems and technology.

The NHSX Parties have also entered into a Joint Controller and Information Sharing Framework Agreement. The NHSX Joint Controller and Information Sharing Agreement can be obtained by emailing england.ig-corporate@nhs.net.

5. Corporate IG team

The work of the Corporate IG team falls into four workstreams. This document defines the responsibilities of each workstream and describes how each activity is undertaken.

5.1 IG delivery



The IG Delivery workstream is responsible for carrying out operational IG activities to ensure we meet our legal and statutory requirements, whilst providing the Data Protection Officer (DPO) with a support function. These activities are explained in more detail below.

IG operating model and framework; maintaining a robust and comprehensive IG framework through a suite of core IG policies, associated procedures, internal processes and guidance (see Appendix D), supporting a network of SIROs, Caldicott Guardians and strategic and operational IG steering and governance groups.

Operational compliance; providing legal compliance activities such as information asset management, bespoke training, management of our fair processing requirements, incident management, processing of subject access requests and DPO enquiries, responses to ICO requests to meet legal and NHS mandated requirements (see Appendix E).

Regional IG; supporting our regional staff, SIROs and Caldicott Guardians to maintain compliance with data protection requirements, providing regionally allocated subject access request responses, reviewing incidents and providing compliance reporting to regional colleagues to provide continuous improvement through identification of incident trends and lessons learned.

Data Security and Protection (DSP) Toolkit; related to operational compliance, providing an action plan and ensuring stakeholder engagement to collate and submit evidence to provide compliance with the annual DSP toolkit.

DPO support function; a triage service through a dedicated mailbox for subject rights requests providing a personal, targeted and efficient service to monitor responses within statutory timescales, triaging and managing responses to ICO enquiries requiring formal or informal action.

Corporate IG mailbox; a dedicated mailbox for all IG enquiries and support requests, which is monitored Monday to Friday during core working hours.

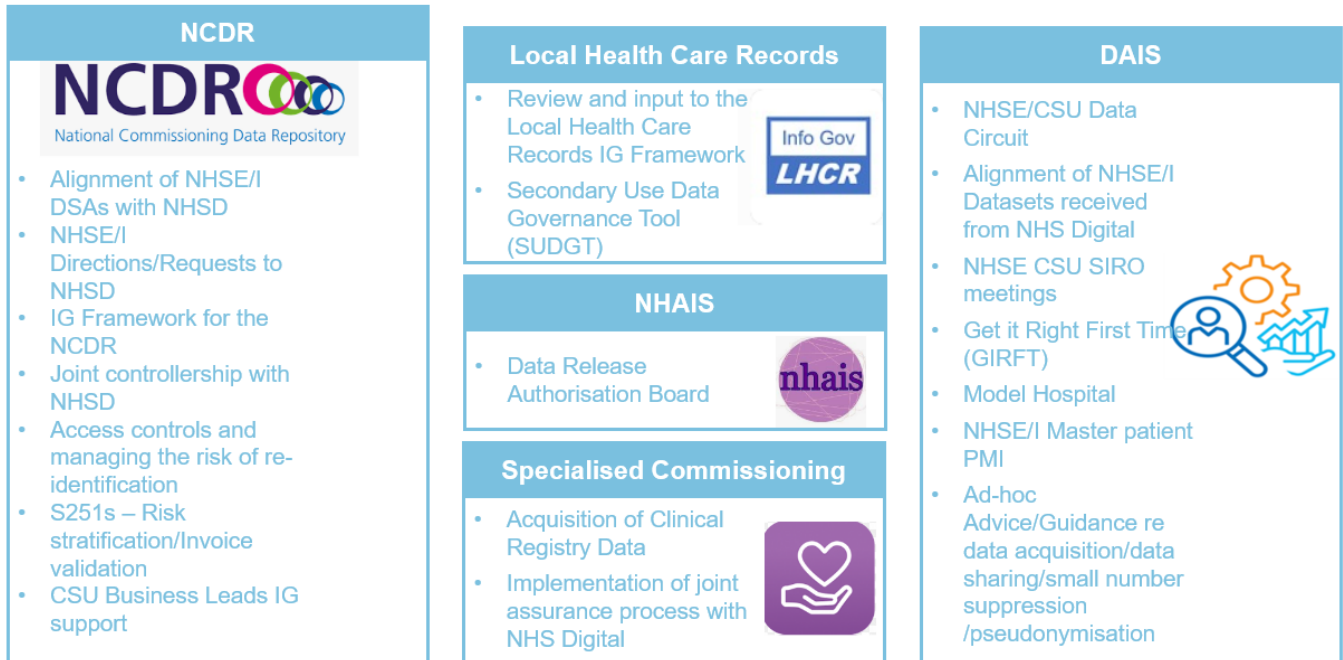
Data Protection Impact Assessments (DPIAs); we have a legal duty to undertake appropriate, prior assessment to confirm that implementation of new processes, services, systems and information assets are introduced, or significant changes to existing systems, that involve the processing of personal data, do not result in an adverse impact on privacy, information quality or a breach of information security, confidentiality or data protection requirements.

Information asset management system (IAMS); we must update and maintain our information asset register to ensure we meet the legal requirement under GDPR to hold a register of our processing activities. An information asset is any piece or collection of information that holds data. Assets have recognisable and manageable value, risk, content and lifecycles and can range from a basic excel spreadsheet to a national system. Our information asset register identifies the different types of information processed, stored and communicated. We need to achieve and maintain appropriate protection of information assets to ensure we have a legal basis to process the data. Information assets are managed through a network of information asset owners and administrators throughout the organisation.

Information security incident reporting and monitoring; supporting the online incident reporting portal, ensuring we comply with our legal obligation to report all notifiable incidents within 72 hours, monitoring trends both in incident types and areas of the business, identifying threats to services or systems.

Operational IG risk and issue management and monitoring; providing an IG risks and issues framework, providing assurance to the National IG Steering Group and SIRO that appropriate processes are in place for monitoring and reporting IG risks and issues.

5.2 Data governance



The Data Services for Commissioners (DSfC) programme was 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. The DSfC programme has now transitioned into the Data, Analysis & Intelligence Service (DAIS). 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.

The DAIS team manages the NHS England and NHS Improvement data repositories, namely NHS England's National Commissioning Data Repository (NCDR) and NHS Improvement's Strategic Information Platform (SIP). As these are corporate information assets, they require a significant amount of business as usual IG processes, and as such it was agreed that the Corporate IG team would provide dedicated IG support for this team.

One of the DAIS team areas is to support NHS England and NHS Improvement analysts so that they receive the data they require to ensure the joint organisations can meet their statutory duties.

The support provided by the Data Governance team also extends to working with CCGs, Local Authority 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.




Commissioners can only receive data which has been anonymised in accordance with the Information Commissioner's 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 DAIS team also requires specific IG support in relation to the following key areas:

- Alignment of NHS England and NHS Improvement data repositories and consequently the acquisition of data from NHS Digital;
- Working with NHS Digital to implement a joint controller agreement in line with responsibilities under GDPR/Data Protection Act 2018 when NHS England and NHS Improvement issue mandatory directions or requests for data to NHS Digital;
- Amendment of the current NHS Digital Data Sharing Agreements with NHS England or NHS Improvement in relation to data;
- Supporting the NHS England CSU Business Leads with IG support and guidance in relation to NHS England and NHS Improvement's Unified Data Access Layer (UDAL), previously known as the Data Circuit, which will be using cloud technology to process data across all NHS England CSUs;
- Working with NHS Digital, the ICO and other stakeholders to develop updated guidance for organisations applying pseudonymisation and anonymisation techniques to data ensuring there are wider technical and business controls to protect data. Supporting NHS Digital in the 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 CSUs/CCGs under s251 of the NHS Act 2006;
- Undertaking audits of CSUs to ensure that they have appropriate data processing agreements in place with the commissioners they are providing services to;
- Providing dedicated support to the specialised commissioning team to obtain clinical registry data. This has necessitated the implementation of an assurance process to undertake due diligence on the clinical registries themselves to ensure they are processing data lawfully.

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

5.3 Records and information management

Current Records	Programmes
<p>We provide tools for staff to manage their records; (policies, guides, mandatory training, RIMCs) answer queries, produce various publications, advise on systems in place</p> 	<ul style="list-style-type: none"> • PCS legacy records • Corporate legacy records • Electronic Records Management Design, implementation and management of <ul style="list-style-type: none"> • Electronic Records Management System • Covid Records Management System 
Statutory and Public Inquiries	Covid 19 Response
<ul style="list-style-type: none"> • Independent Inquiry into Child Sexual Abuse, • Infected Blood Inquiry • Gosport • Grenfell • SATH Maternity Review • Impending Covid 19 Statutory Inquiry 	<p>Full team deployed to the Covid 19 response to train staff on RM principles, behaviours & practices.</p> <p>Preparing staff and their records, so the organisation is in a good place to respond to legal e/inquiries by auditing and ensuring learning has been implemented.</p>

Specialist records management advice and guidance is provided by the Corporate Records Management team within Corporate IG. The Corporate Records Management team is responsible for providing professional expertise and the tools needed for staff across NHS England and NHS Improvement to manage their department and directorate records effectively. We create, maintain and promote the Corporate Document and Records Management Policy and the Corporate Records Retention and Disposal Schedule, ensuring that the policy and schedule reflects external policy in the public sector.

User friendly records management guidance is provided for all staff via the intranet, advising on the creation, maintenance, storage, retention and disposal of records within NHS England and NHS Improvement. A bespoke, online records management training package (990 Records Management) now forms part of the mandatory and statutory (MaST) training schedule.

We support legal requests for records such as Reviews, Investigations and Inquiries, and share lessons learnt with the wider organisation.

Records management queries can be received via telephone or email (england.ig-corporate@nhs.net) and these are responded to as soon as possible. On average the team maintain a response rate of between 1 – 2 working days. Queries are maintained in a log for future reference.

The Corporate Records Management team has responsibility for promoting and managing the use of the [Electronic Records Management System \(ERMS\)](#), which stores current organisational records and has been located on the NHS England intranet since August 2016 and latterly, also on the NHS Improvement intranet. An updated ERMS is currently being investigated to meet the needs of both NHS England and NHS Improvement's corporate records requirements.

As well as having responsibility for current records, NHS England and NHS Improvement inherited thousands of corporate records from the closed Primary Care Trusts (PCTs) and

Strategic Health Authorities (SHAs), which ceased to exist in April 2013. The allocation of these records was managed by DHSC. These records are known as legacy records and the Corporate Records Management team receives numerous queries, Freedom of Information requests and subject rights requests for these legacy records on a regular basis. Additionally, these legacy records play a vital part in providing evidence for various statutory and public inquiries. These records are stored in paper format at storage facilities throughout England and the team maintain inventories for these records on an SQL database.

Primary Care Support England (PCSE) legacy records, also inherited from the former PCTs and SHAs, were previously managed by a PCSE team however these records are currently in the process of being transferred to the Corporate Records Management team to manage through their lifecycle.

Regular audits of current records are undertaken in accordance with the Records Management Audit Framework and the Information Governance Alliance's Records Management Code of Practice 2016. These audits are undertaken by the Corporate Records Management team who report their findings to the Corporate Teams IG Operational Group (CTIGOG).

Records and Information Management Co-ordinators (RIMCs) have been in place in NHS England since 2013, and as a joint network with NHS Improvement since 2019. They are responsible for promoting records management within their teams, cascading advice and guidance to members of their teams, and declaring records within the ERMS. RIMCs receive full training and induction from the Corporate Records Management team in addition to online Yammer group/Microsoft Teams chats. There is also a bi-monthly meeting for RIMCs, which is delivered via MS Teams. This meeting informs RIMCs of the latest developments in records management and also offers an opportunity for RIMCs to discuss local issues in a supported forum. The terms of reference for the group can be found [here](#). In between meetings, a bi-monthly bulletin for RIMCs is produced, advising them of the latest news, in terms of records management activities and planned developments.

5.4 IG Assurance and Planning

Assurance	Comms and Engagement	Planning
<p>Provides pro-active assurance to the DPO and Boards of ongoing data protection compliance</p> <ul style="list-style-type: none"> Assuring GDPR/DPA compliance of: <ul style="list-style-type: none"> NHSE/I Teams CSUs Hosted Bodies Data Processors Reviewing and proposing improvements to: <ul style="list-style-type: none"> Corporate systems and frameworks Policies Procedures Operating Processes Reporting organisational compliance to IG SMT, SIRO, CTIG, NIGSG and Corporate Exec 	<p>Ensures consistent regional and national IG communications deliver a single corporate message</p> <ul style="list-style-type: none"> Developing and implementing the national IG engagement strategy Planning, recording and co-ordinating IG communications Preparing IG newsletters, blogs and articles for corporate communications Planning and co-ordinating annual IG week Developing IG branding Maintaining IG intranet Reviewing effectiveness of IG communications 	<p>Enables Corporate IG resources to be prioritised, co-ordinated and allocated effectively</p> <ul style="list-style-type: none"> Establishing and maintaining team Planner boards to effectively capture team capacity and priorities Developing and consolidating PMO reporting for IG SMT, TCD leadership team and Corporate Exec Leading on annual prioritisation and business planning cycles Monitoring and managing Corporate IG budgets Supporting recruitment activities 

The IG assurance and planning workstream has three main objectives:

- IG assurance**; in line with GDPR's new accountability principle, dedicated IG Assurance staff seek pro-active assurance of NHS England, NHS Improvement and NHSX compliance with IG legislation, codes of conduct and best practice, spanning data protection, information security and records and information management. This is achieved through a rolling programme of compliance deep dive reviews with our teams, hosted bodies and data processors to identify and implement improvements to local IG practices and provide compliance assurance to the Data Protection Officer (DPO) and board. The team also continually monitor the effectiveness of our corporate frameworks, policies, procedures and processes to ensure they maximise IG compliance, identify any risks and propose improvements where required.
- IG engagement**; the workstream is responsible for establishing and delivering an effective IG communications, awareness and engagement strategy to maintain IG awareness across our organisation. Through this strategy, all IG communications to the business are co-ordinated and key messages cascaded through a variety of mediums, including newsletters, intranet sites, blogs and videos, as well as face to face engagement.
- IG programme management office (PMO)**; The PMO team ensures that Corporate IG's objectives are effectively resourced, prioritised and reported through a robust project management function that co-ordinates project activities and planning across all Corporate IG workstreams. It provides reporting to the IG Senior Management Team, the Commercial Directorate Senior Leadership Team and Corporate Executive. The team also delivers administrative aspects of the function including annual business planning and budget management.

5.5 Primary Care Support England (PCSE)

NHS England is responsible for providing primary care support functions and Capita has 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.

The Corporate IG Team provides IG support and oversight to PCSE by monitoring their compliance with the Data Protection Act 2018, the Data Security and Protection (DSP) Toolkit, incident management and by providing ad hoc advice on information disclosures. The IG Assurance and Planning team provides strategic oversight and assurance of PCSE's IG processes and activities, while the IG Delivery team supports PCSE to resolve operational IG queries and issues.

There is a monthly PCSE and NHS England IG Operational Group co-ordinated by the NHS England and NHS Improvement Service Management Team and this group is responsible for:

- Ensuring that there is clarity around the operational IG requirements of PCSE;
- Ensuring that the IG Operating Model is updated as and when required;
- Monitoring adherence with the IG Operating Model, including high-level monitoring of DSP Toolkit completion;
- Providing a forum for IG operational issues to be raised by Capita, NHS England and NHS Improvement or Public Health England;
- Establishing 'task and finish' sub-groups for any specific IG related issues;
- Providing an overview of Capita's transformation programme and associated IG issues;
- Review and feedback of data protection impact assessments and other IG documents related to PCSE services;
- Monitoring of IG incidents in PCSE; and
- Review of IG risks in PCSE.

6. IG Policy team (NHSX)

The NHSX IG Policy team, previously known as the Data Sharing Privacy Unit, sits within the NHSX, Policy and Strategy Directorate, under the Directorship of Simon Madden. NHSX leads the digital transformation agenda and the IG policy team provides IG support for those programmes and initiatives.

IG Policy assists in delivering the Health Secretary's Tech Vision, building on the long-term plan and meeting the programme priorities. They are tasked with expediting the digital transformation of the NHS and social care by supporting the delivery of NHSX missions in particular, reducing burden, improving productivity and ensuring appropriate access to information.

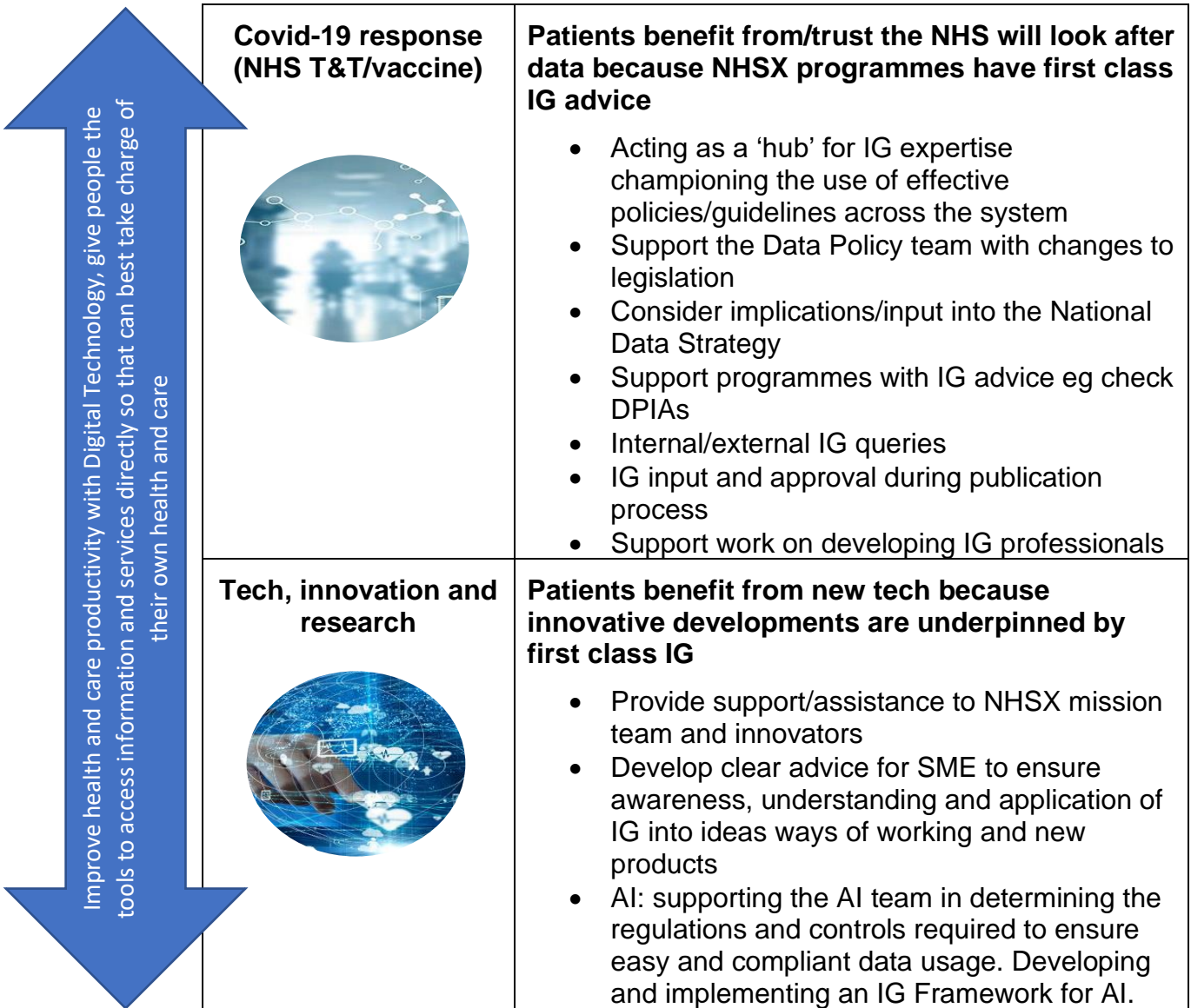
They do this by the coordination and consistency of national policy for data sharing and transparency, developing and publishing good practice guidance through the Health and Care IG Panel to front line staff, IG professionals and the public.

The team also has responsibilities for developing, agreeing and managing clear information governance standards.

The NHSX IG Policy team is responsible for proactively identifying and understanding system wide IG issues within the Health and Social Care sector and ensuring that IG strategy and policy is developed and implemented to meet the needs of our external stakeholders.

6.1 Programmes of work and workstreams

	<p>Simplification of IG</p>	<p>Information is shared appropriate to improve care because NHSX provides clear/consistent IG advice</p> <ul style="list-style-type: none"> • Provide Secretariat for Health & Social Care Information Governance Panel • Develop operating model for Health & Social Care Information Governance Panel • Update and simplify existing guidance targeting audiences to ensure better awareness and understanding • Audit published guidance across the system to ascertain baseline requirements • Launch NHSX Portal IG pages, deliver a One Stop Shop
	<p>EU Exit</p>	<ul style="list-style-type: none"> • Lead IG messages and approach to data transfers post EU Exit • Delivering webinar and other targeted communications • Monitoring Assurance • Represent Data Workstream at Executive Board Meetings and operational boards • Work in alignment with the NCC and EU Exit team
	<p>Joining up of care (Primary Care and Social Care)</p>	<p>Information is shared appropriate to improve the care of patients and service users to improve care</p> <ul style="list-style-type: none"> • Further develop socialise, and publish the IG Framework for integrated care in line with open values and ensure the framework meets the needs of ICS/STPs • Develop and resolve policy issues and gain agreement of IG policy lines relating to integrated care • Develop social care stakeholder group to understand priority IG areas for resolution • Secure awareness and understanding within the social care section of the National Data Opt Out • Build an understanding of the need to apply the common law duty of confidentiality across the social care sector



7. Governance framework

7.1 Roles and responsibilities

7.1.1 SIRO framework

The Chief Commercial Officer is the National SIRO for NHS England and NHS Improvement. Deputy SIROs are appointed across the corporate team, each region and CSUs to support the National SIRO, who they are accountable to.

7.1.2 Deputy SIROs

Deputy SIROs undertake the general roles and responsibilities of a SIRO but at a regional/corporate/CSU level, escalating any risks or issues to the National SIRO. Deputy SIROs are responsible for approval of data protection impact assessments and risk assessments for regional and CSU assets. Further information regarding their role and responsibilities can be found at Appendix F.

Regional deputy SIROs and CSU deputy SIROs chair their IG operational groups and attend the National IG Steering Group.

SIROs 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 skills and capabilities are up to date and relevant to the needs of the organisation and to ensure they remain effective in the role.

Further information regarding their role and responsibilities can be found at Appendix G.

7.1.3 Caldicott Guardians

The National Medical Director is the National Caldicott Guardian. Caldicott Guardians have also been appointed in regional teams and CSUs and are accountable to the National Medical Director.

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

Regional Caldicott Guardians are key stakeholders in data protection impact assessments where there is any processing of patient data and are responsible for approval of information sharing agreements and data processing agreements that contain patient data and local information disclosure requests. A centralised log of Caldicott requests and decisions is maintained within our IG Advice Register to ensure consistency across the organisation.

Further information regarding their role and responsibilities can be found at Appendix G.

The regional Caldicott Guardians attend regional IG operational groups and the National IG Steering Group.

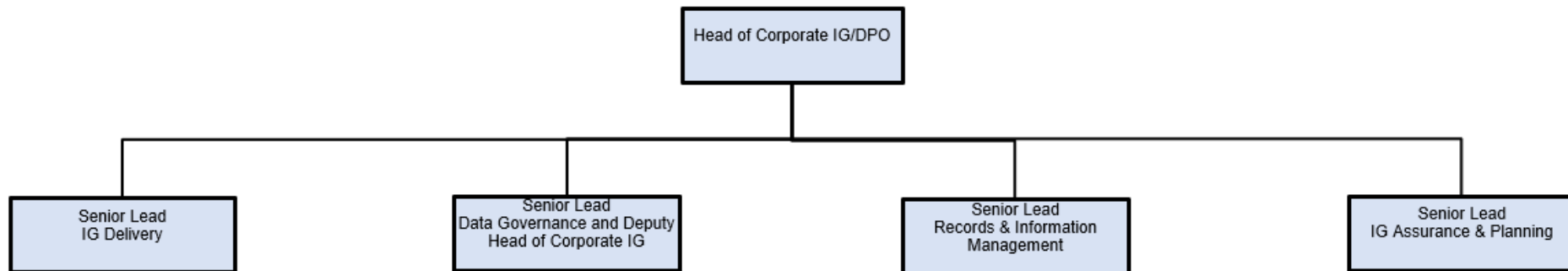
Caldicott Guardians should review the UK Caldicott Guardian Council website regularly to ensure they remain aware of current guidance and effective in the role, relevant to the needs of the organisation. Any specialist training will be assessed as part of the annual review of our training needs analysis for data protection.

7.1.4 Meeting structure

To ensure we deliver organisational IG objectives, we have a formal meeting structure in place. Regional operational IG groups are held across the seven regions, with attendance by regional IG managers, SIROs and Caldicott Guardians. Similarly, a Corporate Teams IG Operational Group is held quarterly. These feed into the National IG Steering Group, which in turn, regularly reports to the Corporate Executive team on key objectives and risks.

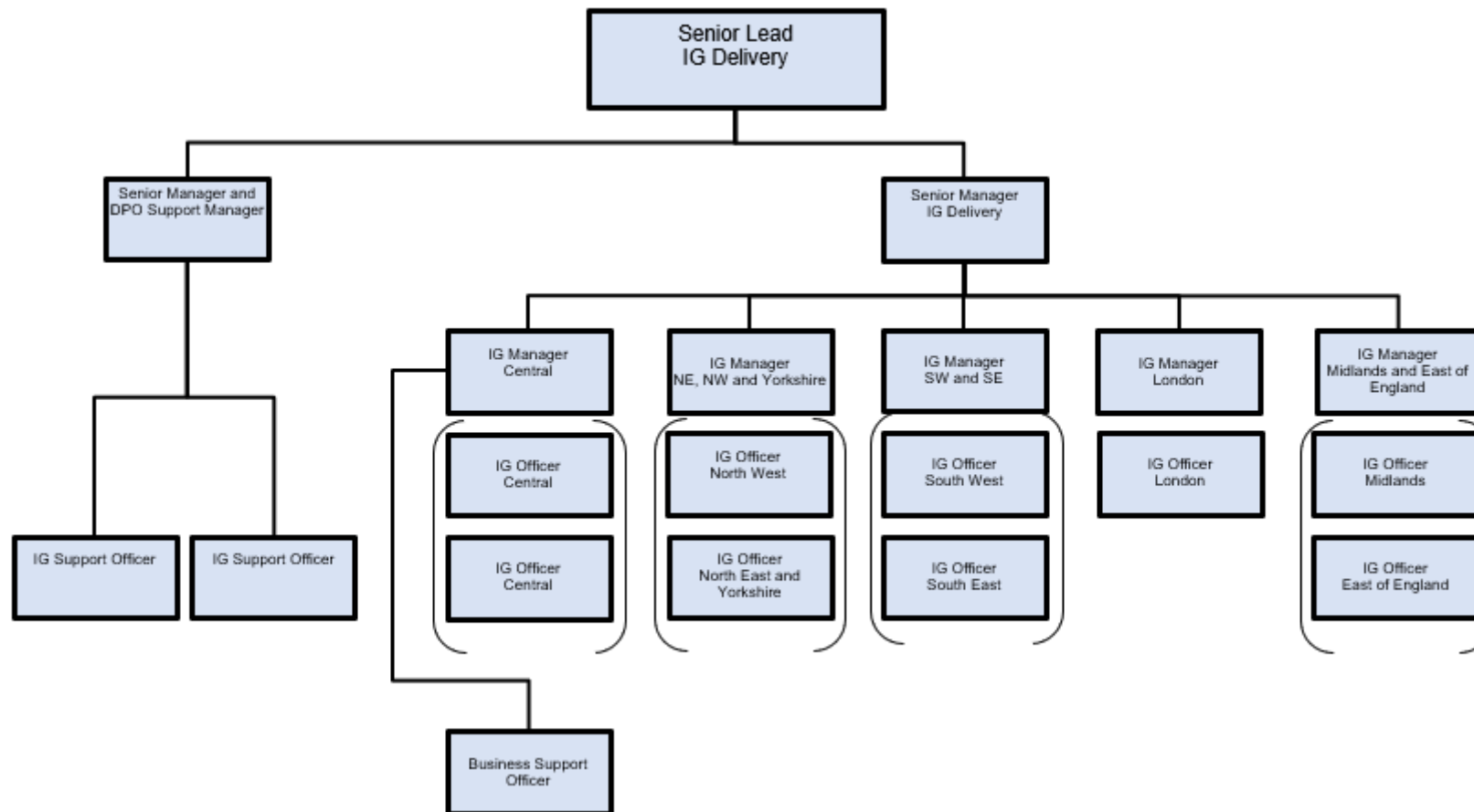
Appendix A – Corporate IG structure

Senior Management Team



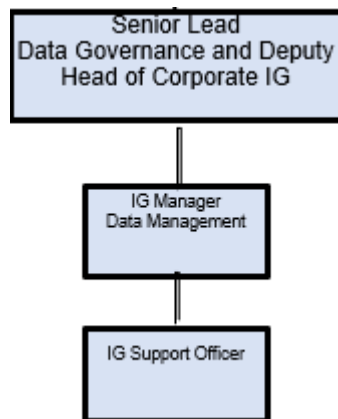
Corporate IG structure continued

IG Delivery

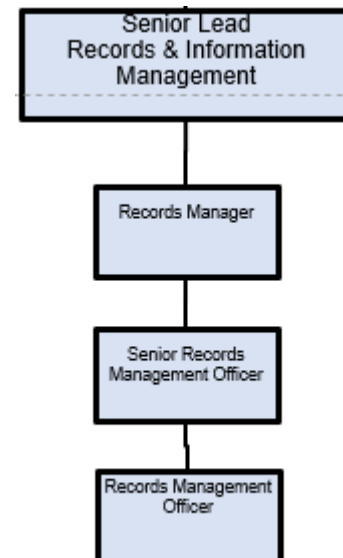


Corporate IG structure continued

Data Governance

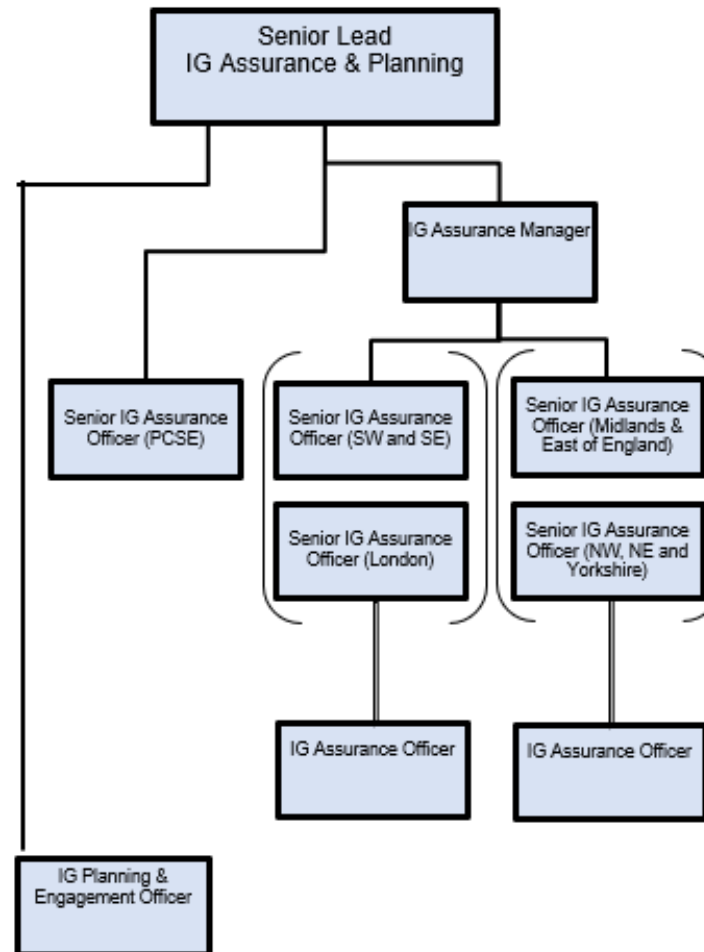


Records and Information Management



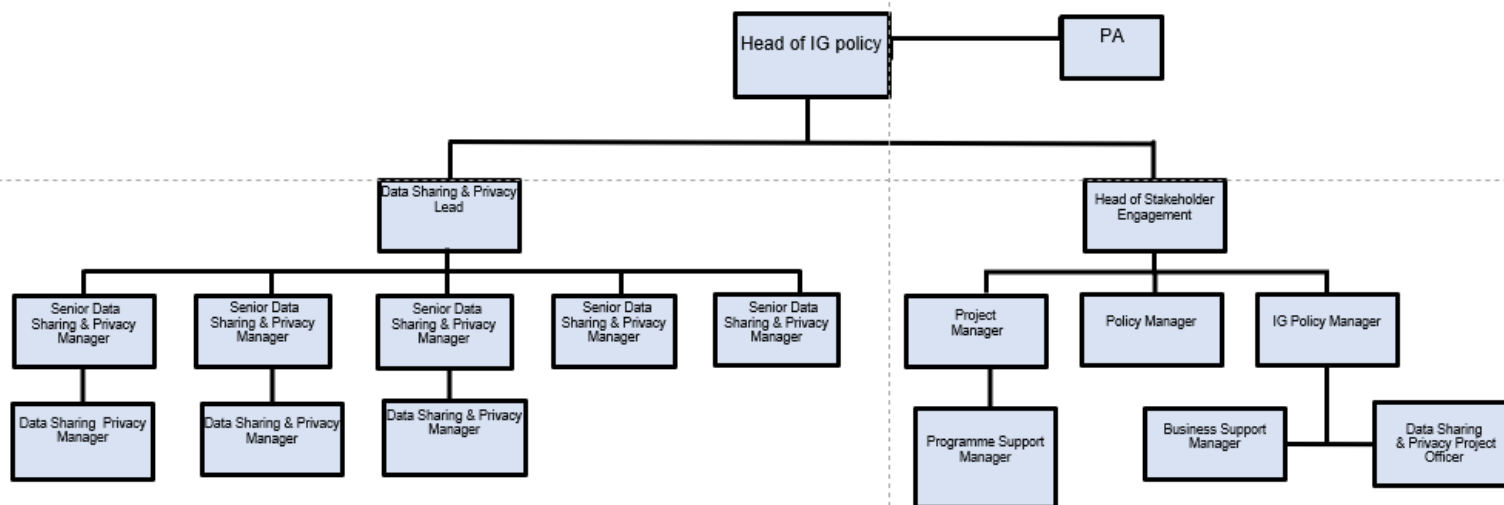
Corporate IG structure continued

IG Assurance and Planning



Appendix B – IG Policy team structure

Information Governance Policy Team



Appendix C – IG accountability and responsibilities

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 key legal responsibilities are set out below:

- i. NHS England must itself comply with the legal framework governing the use of information in the exercise of its powers. 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 1998. NHS England also has responsibility for commissioning of primary and specialised care services and for holding such providers to account for the services provided including the effective and lawful use of personal and confidential information.
- ii. NHS England's duties to exercise its functions efficiently and effectively, and with a view to securing continuous improvement in the quality of services, 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.
- iii. NHS England must publish guidance on the processing of information to providers registered with the CQC, across both health and social care;
- iv. NHS England must publish guidance on commissioning for CCGs for which IG is a key component;
- v. NHS England alongside the Secretary of State has responsibility for information standards, which include those related to IG;
- vi. 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 purposes;
- vii. NHS England is also under an obligation to promote the NHS Constitution which includes key requirements in relation to the use of patient information;
- viii. NHS England is empowered to issue directions to NHS Digital and others to enable the lawful flow of data where permitted through its statutory functions.

NHS Improvement's key legal responsibilities for information governance are:

- i. Internal compliance and assurance
NHS Improvement which is made up of Monitor, the NHS Trust Development Authority (NHS TDA) and hosted bodies, must comply with the legal framework governing the use of information in the exercise of its powers, ensuring its own internal compliance with

legal requirements which includes a positive obligation as a public body to protect and promote the privacy of individuals under the Human Rights Act 1998.

- ii. **Mandate**
The Mandate from the Government sets out the list of requirements for Monitor and NHS TDA to fulfil each year. Many of these activities involve the use of data and therefore IG is essential to ensure the lawful and effective use of such information to achieve these purposes.
- iii. **NHS Constitution**
Monitor and NHS TDA are under an obligation to promote the NHS Constitution which includes key requirements in relation to the use of information.
- iv. **Directions**
Monitor and NHS TDA are empowered to issue directions to NHS Digital to collect information where required to fulfil their functions.

Appendix D – Policies and procedures

IG management framework and strategy	
Policies	Procedures
<ul style="list-style-type: none"> • Acceptable Use of ICT and User Obligations Policy • Information Security Policy • System Level Security Policy • Confidentiality Policy • Corporate Document and Records Management Policy • Information Governance Policy • Data Protection Policy • Information Sharing Policy • Processing of Personal Data Outside of the UK (Offshoring) Policy 	<ul style="list-style-type: none"> • Information Asset Management Procedure • Information Security Incident Reporting Procedure • New Personal Data Processing Procedure • Safe Haven Procedure • Risk and Issue Management Procedure • DPO Risk Management and Escalation Procedure • Procedure for Managing Personal Data Requests • Corporate Records Retention and Disposal Schedule • Missing Records Procedure

Confidentiality Policy

Lays down the principles that must be observed by all who work within NHS England and NHS Improvement and have access to personal or confidential business information. All staff must be aware of their responsibilities for safeguarding confidentiality and preserving information.

Corporate Document & Records Management Policy and Retention Schedule

This policy is to promote the effective management and use of information, recognising its value and importance as a resource for the delivery of corporate and service objectives.

Data Protection Policy

Sets out the roles and responsibilities for compliance with the Data Protection Act (2018).

Information Governance Policy

Helps the people who work for NHS England and NHS Improvement to understand how to look after the information they need to do their jobs, and to protect this information on behalf of patients.

Information Security Policy

This policy is to protect, to a consistently high standard, all information assets. The policy defines security measures applied through technology and encompasses the expected behaviour of those who manage information within the organisation.

Information Sharing Policy

The policy ensures that all information held or processed by NHS England or NHS Improvement is made available subject to appropriate protection of confidentiality and in line with the terms and conditions under which the data has been shared with NHS England or NHS Improvement. This policy sets out what is required to ensure that fair and equal access to information can be provided and is supported by a range of procedures.

Processing Personal Data Outside of the UK (Offshoring) Policy

This policy helps those who work for NHS England and NHS Improvement understand how to securely and legally process personal data outside of the United Kingdom.

Appendix E – Legal and NHS mandated frameworks

NHS England and NHS Improvement are obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of NHS England and NHS Improvement, who may be held personally accountable for any breaches of information security for which they may be held responsible. NHS England and NHS Improvement shall comply with the following legislation and guidance as appropriate:

The **Data Protection Act (2018)** regulates the use of “personal data” and sets out eight principles to ensure that personal data is:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and where necessary kept up to date.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Caldicott Report (1997) and subsequent Caldicott or National Data Guardian reviews recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared:

- Justify the purpose for using patient-identifiable information.
- Don't use patient identifiable information unless it is absolutely necessary.
- Use the minimum necessary patient-identifiable information.
- Access to patient-identifiable information should be on a strict need to know basis.
- Everyone should be aware of their responsibilities.
- Understand and comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality.

See the [Information Governance Review](#) and the [Department of Health response](#).

Human Rights Act (1998); Article 8 refers to an individual's “right to respect for their private and family life, for their home and for their correspondence”. This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

The [Computer Misuse Act \(1990\)](#) makes it illegal to access data or computer programs without authorisation and establishes three offences, together with making, supplying or obtaining articles for use in offences 1-3:

1. Unauthorised access to data or programs held on a computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.
3. Unauthorised acts with intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

The [NHS Confidentiality Code of Practice \(2003\)](#) outlines four main requirements that must be met in order to provide patients with a confidential service:

- Protect patient information.
- Inform patients of how their information is used.
- Allow patients to decide whether their information can be shared.
- Look for improved ways to protect, inform and provide choice to patients.

Common Law Duty of Confidentiality; Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

Administrative Law; Administrative law governs the actions of public authorities. According to well established rules a public authority must possess the power to carry out what it intends to do. If not, its action is “ultra vires”, i.e. beyond its lawful powers.

The NHS Care Record Guarantee; The Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to: patients’ rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made. The most relevant are:

- Commitment 3 - We will not share information (particularly with other government agencies) that identifies you for any reason, unless:
 - You ask us to do so.
 - We ask, and you give us specific permission.
 - We have to do this by law.
 - We have special permission for health or research purposes; or
 - We have special permission because the public good is thought to be of greater importance than your confidentiality, and
 - If we share information without your permission, we will make sure that we keep to the Data Protection Act, the NHS Confidentiality Code of Practice and other national guidelines on best practice.

- Commitment 9 - We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policies and controls as the NHS does. We will enforce this duty at all times.

Appendix F – SIRO roles and responsibilities

The Senior Information Risk Owner (SIRO) will be a National Director and Board Member who will take overall ownership of the organisation's policy on managing information risk, act as champion for information risk on the Board and provide written advice to the Accounting Officer on the content of the organisation's annual governance statement in regard to information risk.

The SIRO will implement and lead the NHS IG risk assessment and management processes within the organisation and advise the Board on the effectiveness of information risk management across the organisation.

The SIRO is expected to understand how the strategic business goals of the organisation may be impacted by information risks, and how those risks may be managed.

The SIRO shall receive training as necessary to ensure they remain effective in their role as Senior Information Risk Owner.

SIRO key roles and responsibilities

Information risk policy and process

- To be accountable to the NHS England and NHS Improvement Board for the management of information risks within the organisation (including CSUs) and for holding Information Asset Owners to account for the management of information assets and related risks and issues within their respective remits.
- To have devolved responsibility to act on behalf of the Board to ensure that IG and cyber security requirements of NHS England and NHS Improvement are fulfilled.
- To take ownership of the organisation's policy on information risk, ensuring effective implementation and compliance with NHS IG policy and standards.
- Review and agree actions in respect of identified information risks and issues.
- To oversee compliance with regulatory, statutory and organisational information and cyber security policies and standards, including oversight of assurance of CSUs, information and cyber security.
- To advise the Board and Accounting Officer on the potential impact of information risks and issues from across the organisation and its business partners on NHS England and NHS Improvement's strategic objectives and policy.
- To advise the Board on the effectiveness of information risk management across the organisation.
- To provide written advice to the Accounting Officer on the content of the organisation's annual governance statement with regard to information risk.

Incident Management

- To ensure that there are effective mechanisms in place for reporting and managing data security and protection incidents relating to the information of the organisation that supports the sharing of lessons learnt.

- Provide assurance to the Board that corporate incidents are monitored and investigated appropriately, including CSU incidents.

Leadership

- To provide a focal point for the escalation, resolution and discussion of information risks and issues.
- Provide leadership for corporate and regional deputy SIROs and IAOs of the organisation through effective networking structures, sharing of relevant experience, provision of training and creation of information risk reporting structures.
- Identify and maintain a network of deputy SIROs as a framework of adequate support to the organisation.
- To champion information risk on the Board.

Deputy SIRO key roles and responsibilities

Deputy SIROs have been appointed corporately and within each region to support the National SIRO.

They will undertake the general role and responsibilities of a SIRO but at a regional level and escalate any risks or issues to the National SIRO as described in the Risk and Issue Management Procedure.

Deputy SIROs will represent their region at the National IG Steering Group.

Deputy SIROs shall receive training as necessary to ensure they remain effective in their role.

Information risk policy and process

- Review and agree actions in respect of identified information risks and issues.
- Ensure the region adheres to the organisation's policy on information risk.
- To escalate risks in accordance with the Risk and Issue Management Procedure.
- To have oversight that regional information assets are recorded within the IAM system and that they are managed in accordance with the Information Asset Management procedure by receiving and reviewing the SIRO report and taking action as necessary
- Review and approve regional DPIAs for new projects and services or where there are significant changes to current processing.
- To provide a focal point for resolution of identified IG issues.
- To receive IG assurance reports from deep dives to enable best practice and lessons learnt to be shared and to ensure actions are completed.
- Oversight of information handling activities to ensure regional compliance with the law and guidance (GDPR, FOI, EIR and AHRA requests).
- To review and monitor IG risks and issues identified on the risk register.
- Oversight of new risks or issues entered onto the risk register and escalated as per the Risk and Issue Management Procedure.

Incident management

- Be a point of escalation for data security and protection incidents in the region.
- Ensure region incidents are reported and managed in accordance with the Risk and Incident Management Procedure.
- Oversight of security incident reports and root cause analyses carried out, remedial action and lessons learnt.

Leadership

- Champion information risk in the region.
- Provide a focal point for the escalation, resolution and discussion of information risks and issues.
- Provide leadership for IAOs of the organisation through effective networking structures, sharing of relevant experience.
- To support the cascade of key IG messages to staff in the region.

SIROs and Deputy SIROs within CSUs and hosted bodies

Roles and responsibilities are defined in the Deputy DPO Risk Escalation Procedure available from england.ig-corporate@nhs.net.

Appendix G – Caldicott Guardian roles and responsibilities

Caldicott Guardians are an integral part of our organisation's arrangements for information governance. Their primary concern is who should be able to access personal information, working as part of the broader IG function, working closely with the IG team.

Context of the role

The Caldicott Guardian is a senior role within our organisation which makes sure that the personal information about those who use our services is used legally, ethically and appropriately, and that confidentiality is maintained. Caldicott Guardians should be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing.

The Caldicott Guardian should play a key role in ensuring that our organisation satisfies the highest practical standards for handling personal-identifiable information. Their main concern is information relating to patients, service users and their care, but the need for confidentiality extends to other individuals, including their relatives, staff and others. Our organisation stores, manages and shares personal information relating to staff, and the same standards will be applied to these as to the confidentiality of patient information.

The Caldicott Guardian will apply the [seven Caldicott principles](#) wisely, using common sense and an understanding of the law. They are compassionate, recognising that their decisions will affect real people. The importance of the Caldicott Guardian acting as 'the conscience of the organisation' remains central to trusting the impartiality and independence of their advice.

The Caldicott Guardian also has a strategic role which involves representing and championing IG requirements and issues at senior management team and board level and, where appropriate, throughout our organisational governance framework, including the governance of information management and technology. This aspect of the Caldicott Guardian's role is particularly important in relation to the implementation of the digital agenda.

Regional Caldicott Guardians

Caldicott Guardians have been appointed within each region to support the National Caldicott Guardian.

They will undertake the general role and responsibilities of the Caldicott Guardian but at a regional level and escalate any risks or issues to the National Caldicott Guardian.

Regional Caldicott Guardians will represent their region at the National IG Steering Group.

Caldicott Guardians shall receive training as necessary to ensure they remain effective in their role as Caldicott Guardians.

Responsibilities

The Caldicott Guardian will champion confidentiality issues at board and senior management team level and will attend the National IG Steering Group, acting as both the 'conscience' of our organisation and as an enabler for appropriate information sharing.

The Caldicott Guardian will develop a strong knowledge of confidentiality and data protection matters, drawing upon support from the Corporate IG team, as well as external sources of advice and guidance where available.

They will ensure that confidentiality issues are appropriately reflected in organisation strategies, policies and working procedures for staff as reflected in the requirements of the DSP Toolkit.

The Caldicott Guardian will oversee all arrangements, protocols and procedures where personal information may be shared with external bodies and others with responsibilities for social care and safeguarding. This includes flows of information to and from partner agencies, sharing through IT systems, disclosure for research and disclosure to the police.

Many or all of these responsibilities may be shared with the SIRO, with whom the Caldicott Guardian will work closely.

Accountability

The Caldicott Guardian role has no statutory basis. It was originally conceived as an advisory role. Many information sharing and disclosure scenarios are decided by the Caldicott Guardian and it is important that these are documented.

The National Caldicott Guardian is directly accountable to the Chief Executive.