

# Information Governance Policy



## Information Governance Policy

Version number: v5.1

Updated: September 2019

Prepared by: Corporate Information Governance

Classification: OFFICIAL

This information can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request. Please contact [england.ig-corporate@nhs.net](mailto:england.ig-corporate@nhs.net)

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 2

**NHS England and NHS Improvement INFORMATION READER BOX****Directorate**

Medical	Operations and Information	Specialised Commissioning Strategy & Innovation
Nursing	<b>Trans. &amp; Corp. Dev.</b>	
Finance		

**Publications Gateway****Reference:**

<b>Document Purpose</b>	Policy
<b>Document Name</b>	Information Governance Policy
<b>Author</b>	Corporate Information Governance
<b>Publication Date</b>	September 2019
<b>Target Audience</b>	All NHS England and NHS Improvement Employees
<b>Description</b>	Policy and high-level procedures for Information Governance
<b>Cross Reference</b>	N/A
<b>Superseded Docs</b> (if applicable)	Information Governance Policy v5.0
<b>Action Required</b>	To note
<b>Timing / Deadlines</b> (if applicable)	<b>N/A</b>
<b>Contact Details for further information</b>	Carol Mitchell Head of Corporate Information Governance Quarry House Leeds LS2 7UE
	England.ig-corporate@nhs.net

**Document Status**

This is a controlled document. Whilst the document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 3

## Contents

Contents .....	4
1 Introduction.....	5
2 Purpose .....	6
3 Scope .....	7
4 Roles and Responsibilities .....	7
4.1 Chief Executive .....	7
4.2 Caldicott Guardian .....	7
4.3 Senior Information Risk Owner (SIRO) .....	8
4.4 Data Protection Officer.....	8
4.5 Information Asset Owners.....	9
4.6 Head of Corporate Information Governance .....	9
4.7 Head of Corporate ICT Technology and IT Cyber Security.....	10
4.8 Director of Corporate Operations .....	10
4.9 Line Managers .....	11
4.10 All Staff .....	11
5 Information Governance Policy Framework.....	11
6 National Information Governance Steering Group.....	13
7 Corporate Information Governance Team .....	13
8 Distribution and Implementation .....	14
8.1 Distribution Plan.....	14
8.2 Training Plan.....	14
9 Monitoring.....	14
10 Equality Impact Assessment.....	15
11 Associated Documents .....	15
Version Control Tracker.....	16

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 4

## 1 Introduction

The role of NHS England is to commission healthcare services, both directly and indirectly, so that valuable public resources secure the best possible outcomes for patients. In doing so, NHS England will seek to meet the objectives prescribed in the NHS Mandate and to uphold the NHS Constitution.

NHS Improvement is responsible for overseeing foundation trusts, NHS trusts and independent providers. We offer the support these providers need to give patients consistently safe, high quality, compassionate care within local health systems that are financially sustainable. By holding providers to account and, where necessary, intervening, we help the NHS to meet its challenges and secure its future.

This policy is important because it will help 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 Governance is 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 including:

- Information Governance Management
- Clinical Information assurance for Safe Patient Care
- Confidentiality and Data Protection assurance
- Corporate Information assurance
- Information Security assurance
- Secondary use assurance
- Respecting data subjects' rights regarding the processing of their personal data

The formal framework that leaders of all health and social care organisations should commit to is set out in the National Data Guardian's ten data security standards. These are the basis of the Data Security and Protection Toolkit that health and social care organisations must use to assess their information governance performance.

Under data protection legislation, organisations that process personal data are accountable for, and must be able to demonstrate their compliance with the legislation. The arrangements set out in this and related policies and procedures are intended to achieve this demonstrable compliance.

NHS England and NHS Improvement are cooperating to establish a joint enterprise. This mirrors the focus of the NHS Long Term Plan on how we will deliver integrated care to patients at the local level, how we set the whole of the NHS up to do that and

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 5

how it will benefit patients and communities. To ensure that we comply with our data protection obligations the three statutory organisations (NHS England and NHS Improvement – which comprises Monitor and TDA) have entered into a [Joint Controller and Information Sharing Framework Agreement](#). The Information Sharing Policy sets our framework for processing personal data in support of joint working with reference to this agreement.

## 2 Purpose

The purpose of this policy is to inform NHS England and NHS Improvement staff (permanent or otherwise), including those working for Commissioning Support Units (CSUs), and hosted bodies of their Information Governance responsibilities and the management arrangements and other policies that are in place to ensure demonstrable compliance.

This is the central policy in a suite of policies that informs staff of what they should do:

- To maximise the value of organisational assets by ensuring that NHS England and NHS Improvement demonstrates data is:
  - Held securely and confidentially
  - Processed fairly and lawfully
  - Obtained for specific purpose(s)
  - Recorded accurately and reliably
  - Used effectively and ethically, and
  - Shared and disclosed appropriately and lawfully
  
- To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental. NHS England and NHS Improvement will ensure:
  - Information will be protected against unauthorised access
  - Confidentiality of information will be assured
  - Integrity of information will be maintained
  - Information will be supported by the highest quality data
  - Regulatory and legislative requirements will be met
  - Business continuity plans will be produced, maintained and tested
  - Information governance training will be available to all staff, and
  - All information governance breaches, actual or suspected, will be reported to, and investigated by the Corporate Information Governance team in conjunction with the Data Protection Officer

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 6

### 3 Scope

All our staff and of hosted organisations, without exception, are within the scope of this policy, including and without limitation:

- Central and Regional Teams;
- All Commissioning Support Units;
- NHS Interim and Management Support (NHS IMAS);
- NHS Sustainable Development Unit;
- Strategic Clinical Networks;
- Clinical Senates; and
- Healthcare Safety Investigation Branch (HSIB).

### 4 Roles and Responsibilities

#### 4.1 Chief Executive

Overall accountability for procedural documents across the organisation lies with the Chief Executive as the Accountable Officer that has overall responsibility for establishing and maintaining an effective document management system and the governance of information, meeting all statutory requirements and adhering to guidance issued in respect of information governance and procedural documents.

#### 4.2 Caldicott Guardian

The National Medical Director has been appointed Caldicott Guardian. They will:

- Ensure that NHS England and NHS Improvement satisfies the highest practical standards for handling patient identifiable information
- Facilitate and enable appropriate information sharing and make decisions on behalf of NHS England and NHS Improvement following advice on options for lawful and ethical processing of information, in particular in relation to disclosures
- Represent and champion Information Governance requirements and issues at Board level
- Ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff, and
- Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS

Caldicott Guardians have been appointed in Regions and in all hosted bodies i.e. Commissioning Support Units. These Caldicott Guardians will be accountable to the Medical Director as Senior Responsible Caldicott Guardian for NHS England and NHS Improvement as a whole.

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 7

### 4.3 Senior Information Risk Owner (SIRO)

The National Director of Transformation and Corporate Development has been nominated as Senior Information Risk Owner (SIRO) for NHS England and NHS Improvement. The responsibilities of the SIRO are:

- Take overall ownership of the organisation's Information Risk Policy
- Understand how the strategic business goals of NHS England and NHS Improvement, and how other NHS organisation's business goals may be impacted by information risks, and how those risks may be managed
- Implement and lead the Information Governance Risk Assessment and Management processes within NHS England and NHS Improvement
- Sign off and take accountability for risk-based decisions and reviews in regards to the processing of personal data
- Advise the Board on the effectiveness of information risk management across NHS England and NHS Improvement, and
- Receive training as necessary to ensure they remain effective in their role as SIRO.

Deputy SIROs will also be appointed in Regions and in all CSUs. These SIROs are accountable to the SIRO for NHS England and NHS Improvement.

### 4.4 Data Protection Officer

The Data Protection Officer (DPO) is the Head of Corporate Information Governance, who reports to the SIRO, but also can act independently of the SIRO and report directly to the Board about data protection matters. These may include information governance risks to the organisation, privacy concerns or recommendations with regard to potential changes to, or new initiatives that, involve processing of personal data.

With the support of their office, the DPO will:

- provide advice to the organisation and its employees on compliance obligations with data protection law
- advise on when data protection impact assessments are required
- monitor compliance with data protection law and organisational policies in relation to data protection law
- co-operate with, and be the first point of contact for the Information Commissioner
- be the first point of contact within the organisation for all data protection matters

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 8

- be available to be contacted directly by data subjects
- take into account information risk when performing the above

#### 4.5 Information Asset Owners

Information Asset Owners (IAOs) will:

- Lead and foster a culture that values, protects and uses information for the benefit of patients
- Know what information comprises or is associated with their asset(s) and understand the nature and justification of information flows to and from the asset
- Know who has access to the asset, whether system or information, and why, and ensure access is monitored and compliant with policy
- Understand and address risks to the asset and provide assurance to the SIRO
- Ensure there is a legal basis for processing and for any disclosures, and
- Refer queries about any of the above to the Corporate Information Governance team
- Ensure all information assets they are owner for are recorded on the Information Asset Management System (IAMS) and maintained
- Undertake specialist information asset training as required

#### 4.6 Head of Corporate Information Governance

With the support of the Corporate Information Governance team, the Head of Corporate Information Governance will:

- Maintain an awareness of information governance issues within NHS England and NHS Improvement
- Review and update the information governance policy in line with local and national requirements
- Review and audit all procedures relating to this policy where appropriate on an ad-hoc basis, and
- Ensure that line managers are aware of the requirements of the policy
- Work with the Caldicott Guardian, SIRO and DPO functions to ensure organisational authority and awareness regarding issues relating to data protection or confidentiality concerns.

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 9

## 4.7 Head of Corporate ICT Technology and IT Cyber Security

The role of the Head of Corporate Information Governance is supported by NHS England's Head of Corporate ICT Technology and IT Cyber Security and NHS Improvement's Head of IT and Operational Systems.

The Head of Corporate ICT Technology and IT Cyber Security and Head of IT and Operational Systems are responsible for developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure NHS England and NHS Improvement's systems and infrastructure remain compliant with data protection legislation.

The Head of Corporate ICT Technology and Cyber Security and Head of IT and Operational Systems are responsible for ensuring that all NHS England and NHS Improvement electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.

## 4.8 Director of Corporate Operations

The Director of Corporate Operations is responsible for:

- The formulation and implementation of ICT related policies and the creation of supporting procedures, ensuring these are embedded within the service and developing, implementing and managing robust ICT security arrangements in line with best industry practice;
- Effective management and security of the NHS England and NHS Improvement ICT resources, for example, infrastructure and equipment;
- Developing and implementing a robust IT Disaster Recovery Plan;
- Ensuring that ICT security levels required by the NHS Statement of Compliance are met;
- Ensuring the maintenance of all firewalls and secure access servers are in place at all times, and;
- Acting as the Information Asset Owner for the ICT infrastructure with specific accountability for computer and telephone equipment and services that are operated by corporate and clinical work force, e.g. personal computers, laptops, personal digital assistants and related computing devices, held as an NHS asset.
- Work with the Corporate Information Governance team and DPO office as appropriate regarding matters relating to data and IT security.

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 10

## 4.9 Line Managers

Line managers will take responsibility for ensuring that the Information Governance Policy is implemented within their group or directorate.

## 4.10 All Staff

It is the responsibility of each employee to adhere to this policy and all associated information governance policies and procedures.

Staff will receive instruction and direction regarding the policy from several sources:

- DPO office
- Corporate Information Governance Team
- Policy/strategy and procedure manuals
- Line manager
- Specific training course
- Other communication methods, for example, team meetings; and
- Staff intranet

All staff are mandated to undertake mandatory information governance training in line with the training needs analysis programme as agreed by the National IG Steering Group.

Information governance training is required to be undertaken on an annual basis by all staff.

All staff must make sure that they use the organisation's IT systems appropriately and adhere to the [Acceptable Use of ICT Policy and User Obligations Policy](#).

Section 170 (1) of the Data Protection Act 2018: Unlawful obtaining etc of personal data, states it is an offence for a person knowingly or recklessly:

- (a) to obtain or disclose personal data without the consent of the controller
- (b) to procure the disclosure of personal data to another person without the consent of the controller, or
- (c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

## 5 Information Governance Policy Framework

NHS England and NHS Improvement have developed a framework for their Information Governance Policy. This is supported by a set of Information Governance

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 11

## OFFICIAL

policies and related procedures to cover all aspects of Information Governance which are aligned with the NHS Operating Framework and the Data Security and Protection toolkit requirements.

Associated Information Governance Policies include:

Policies	Description
Data Protection Policy	<i>This policy sets out the roles and responsibilities for compliance with data protection legislation.</i>
Freedom of Information Policy	<i>This policy sets out the roles and responsibilities for compliance with the Freedom of Information Act and Environmental Information Regulations.</i>
Confidentiality Policy	<i>This 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 security in order to comply with common law obligations of confidentiality and the NHS Confidentiality Code of Practice.</i>
Information Security Policy	<i>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</i>
Document & Records Management Policy	<i>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.</i>
Information Sharing Policy	<i>The policy will ensure 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.</i>

Many of these proposals are supported by underpinning procedures. The Information Governance Handbook provides a brief introduction to Information Governance and summarises the key user obligations that support the Information Governance policies and procedures. The IG Handbook must be read and the declaration accepted by every member of staff within the policy scope within the time periods

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 12

defined by the training needs analysis as approved by the Central Team Information Governance Operational Group meeting.

## 6 National Information Governance Steering Group

NHS England and NHS Improvement has established a National IG Steering Group to monitor and co-ordinate implementation of the IG Policy and the Data Security and Protection (DSP) Toolkit requirements and other information related legal obligations. This group is supported by the Central Team IG Operational Group, Regional IG Operational Groups and the CSU IG Leads forum.

## 7 Corporate Information Governance Team

The Corporate Information Governance Team will provide expert advice and guidance to all staff on all elements of Information Governance. The team is responsible for:

- Providing advice and guidance on internal Information Governance to all staff
- Managing the delivery of improvement plans to meet DSP Toolkit assertions.
- Working with NHSX to ensure there is consistency of IG across the organisation and its hosted bodies
- Developing internal IG policies and procedures
- Working with NHSX to establish protocols on how to share information
- Developing IG awareness and training programmes for staff
- Ensuring compliance with Data Protection, Information Security and other information related legislation
- Providing support to the team who handle freedom of information requests
- Implementing Department of Health and Social Care system-wide Information Governance guidance and policy, and
- Providing support to the Caldicott Guardian and Senior Information Risk Owner (SIRO) for internal Information Governance related issues.

The Operations and Information Directorate Data Sharing & Privacy Unit is responsible for:

- Liaison with strategic external stakeholders such as the Department of Health and Social Care, the ICO and the National Data Guardian
- Identifying key strategic IG issues and lead work to analyse problems, find

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 13

solutions and communicate outcomes

- Providing support advice and guidance to internal strategic projects and programmes
- Ensuring responsibility for Information Governance issues is transferred to the Corporate Information Governance team when programmes and projects become established as ongoing business as usual
- Leading on the scoping, commissioning, quality assuring and where appropriate providing Information Governance advice and guidance to the NHS as a whole
- Leading on the scoping, commissioning, quality assuring of Information Governance Standards
- Drafting Directions to NHS Digital as required under the Health and Social Care Act
- Working with the Corporate Information Governance team to ensure there is consistency of Information Governance across the organisation and to establish protocols on how information is to be used (including sharing)
- Working with external stakeholders to ensure consistency of information governance standards and requirements across the health and social care system.

## 8 Distribution and Implementation

### 8.1 Distribution Plan

This document will be made available to all staff via the intranet site. A notice will be issued in the staff bulletin notifying of the release of this document.

### 8.2 Training Plan

A training needs analysis will be undertaken with staff affected by this document.

Based on the findings of that analysis appropriate training will be provided to staff as necessary.

Guidance will be provided on the Transformation & Corporate Development Information Governance intranet site.

## 9 Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Corporate Information Governance team, together with independent reviews by both Internal and External Audit on a periodic basis.

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 14

The Head of Corporate Information Governance is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.

## 10 Equality Impact Assessment

This document forms part of NHS England and NHS Improvement's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

As part of its development this document and its impact on equality has been analysed and no detriment identified.

## 11 Associated Documents

The following documents will provide additional information:

- Acceptable Use of ICT and User Obligations
- Confidentiality Policy
- Corporate Document and Records Management Policy
- Data Protection Policy
- Freedom of Information Policy
- Information Governance Policy
- Information Security Policy
- Information Sharing Policy

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 15

## Version Control Tracker

Version Number	Date	Author Title	Status	Comment/Reason for Issue/Approving Body
1.1	April 2013	Information Governance Senior Manager	Approved	Update the existing policy to reflect the changes in IG responsibilities.
2.0	June 2014	Information Governance Senior Manager		Updated to reflect change of Policy directorate to Transformation & Corporate Operations directorate
3.0	June 2016	Head of Corporate Information Governance		Updated to reflect the changes in job titles and responsibilities.
4.0	August 2018	Data Protection Officer		Updated to reflect new data protection legislation
5.0	March 2019	Data Protection Officer		Aligned with NHS Improvement
5.1	September 2019	IG Manager and Senior Corporate IG Lead	Approved	Amendments to reflect joint working and advice from Counsel and the creation of NHSX

Document Owner: Head of Corporate Information Governance	Prepared by: Corporate Information Governance	First Published:
Document number:	Approval date: 24/9/19	Version number: 5.1
Status: Approved	Next review date: September 2022	Page 16