



Data Protection Policy

Choose an item.

NHS England INFORMATION READER BOX		
Directorate		
Medical	Operations and Information	Specialised Commissioning
Nursing	Trans. & Corp. Ops.	Strategy & Innovation
Finance		
Publications Gateway Reference: 08543		
Document Purpose	Policy	
Document Name	Data Protection Policy	
Author	Corporate IG	
Publication Date	December 2018	
Target Audience	All NHS England Employees	
Additional Circulation List		
Description	Policy and high level procedures for compliance with the Data Protection Act	
Cross Reference		
Superseded Docs (if applicable)	Data Protection Policy v3.0	
Action Required	Compliance	
Timing / Deadlines (if applicable)	N/A	
Contact Details for further information	Corporate Information Governance Quarry House Quarry Hill LS27UE England.ig-corporate@nhs.net	
Document Status		
This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of 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.		

Choose an item.

Data Protection Policy

Version number: 5.0

Updated: August 2018

Prepared by: Corporate IG

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 Corporate IG on england.ig@nhs.net

Contents

Contents	4
1 Introduction.....	5
1.1 Background	5
1.2 Data Protection Principles	5
1.3 Information covered by the Act.....	6
2 Scope	6
3 Roles and Responsibilities	6
3.1 NHS England will:-.....	6
3.2 The Data Protection Officer	7
3.3 Employee Responsibilities.....	7
4 Distribution and Implementation	8
4.1 Distribution Plan	8
4.2 Training Plan	8
5 Monitoring.....	8
6 Equality Impact Assessment	8
7 Associated Documents.....	9
8 Appendix - Local privacy information to be provided when collecting personal data directly from individuals	9
9 Version Control Tracker.....	10

1 Introduction

1.1 Background

NHS England needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include but are not limited to patients, employees (present, past and prospective), suppliers and other business contacts. The information includes name, address, email address, data of birth, private and confidential information, and special categories of personal information. In addition, NHS England may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or other digital media, on hardcopy, paper or images, including CCTV) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 2018 (the Act).

The Act brings the European General Data Protection Regulation (GDPR) in to UK law. References to provisions of the Act in this policy include provisions of the GDPR.

The lawful and proper treatment of personal information by NHS England is extremely important to the success of our business and in order to maintain the confidence of our service users and employees. NHS England must ensure that it processes personal information lawfully and correctly.

1.2 Data Protection Principles

NHS England fully supports and must be able to demonstrate compliance with the six principles of the Act which are summarised below:

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals;
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Personal data processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data shall be 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;

Personal data shall be 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.

Choose an item.

1.3 Information covered by the Act

The Act's definition of "personal data" covers any data that can be used to identify a living individual. Anonymised or aggregated data is not regulated by the Act, providing the anonymisation or aggregation has not been done in a reversible way. Individuals can be identified by various means including their name and address, telephone number or Email address.

The Act defines special categories of personal data (previously referred to as sensitive personal information) as information related to:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sexual history and/or sexual orientation
- Criminal data

2 Scope

Staff within the Scope of this Document

Staff of the following NHS England functions are within the scope of this document:

- Staff working in or on behalf of NHS England (this includes contractors, temporary staff, embedded staff, secondees and all permanent employees);
- NHS England's Commissioning Support Units.

3 Roles and Responsibilities

3.1 NHS England will:-

- ensure that an appropriate framework is in place encompassing relevant roles within the organisation that have responsibility for data protection, including the Data Protection Officer, the SIRO, the Caldicott Guardian and the Head of Corporate Information Governance.
- provide training for all staff members who handle personal information and ensure access to further guidance and support
- provide clear lines of report and supervision for compliance with data protection

Choose an item.

- carry out regular checks to monitor and assess new processing of personal data and to ensure the NHS England notification to the Information Commissioner is updated to take account of any changes in processing of personal data
- develop and maintain Data Protection procedures to include: roles and responsibilities, notification, subject access, training and compliance testing
- Maintain a record of processing activities
- Ensure the organisation complies with its transparency and fair processing obligations in relation to data subjects' personal data

3.2 The Data Protection Officer

As a public authority NHS England is required to appoint a Data Protection Officer by the GDPR. The Information Governance Policy establishes this role. The DPO is responsible for providing advice, monitoring compliance, and is the first point of contact in the organisation for data protection matters. The DPO reports to the SIRO and directly to the Board in relation to data protection matters.

3.3 Employee Responsibilities

All employees will, through appropriate training and responsible management:

- Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information.
- Understand fully the purposes for which NHS England uses personal information.
- Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by the NHS England to meet its service needs or legal requirements.
- Ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required.
- On receipt of a request by or on behalf of an individual for information held about them, or any other data subjects rights in relation to their personal data, staff will immediately notify their line manager and the customer contact centre, and abide by the Procedure for managing personal data requests.
- Not send any personal information outside of the United Kingdom without the authority of the Data Protection Officer.

Choose an item.

- Understand that breaches of this Policy may result in disciplinary action, up to and including dismissal.

4 Distribution and Implementation

4.1 Distribution Plan

This document will be made available to all Staff via the NHS England intranet site.

A link to this document will be provided from the Information Governance intranet site.

4.2 Training Plan

A training needs analysis will be undertaken with Staff affected by this document by the Corporate Information Governance team in conjunction with the Data Protection Officer.

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

Guidance will be provided on the Information Governance intranet site.

5 Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Data Protection Officer and the Information Governance team, together with independent reviews from Internal Audit.

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.

6 Equality Impact Assessment

This document forms part of NHS England'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.

Choose an item.

7 Associated Documents

The following documents will provide additional information:

REF NO	DOC REFERENCE NUMBER	TITLE
		Freedom of Information Policy
		Information Governance Policy
		Confidentiality Policy
		Document and Records Management Policy
		Information Security Policy
		Information Sharing Policy

8 Appendix - Local privacy information to be provided when collecting personal data directly from individuals



Local Privacy
Information Guidance

Choose an item.

9 Version Control Tracker

Version Number	Date	Author Title	Status	Comment/Reason for Issue/Approving Body
1.0	April 2013	Information Governance Senior Manager	Approved	New policy
2.0	June 2014	Information Governance Senior Manager	Approved	Updated to reflect change of Policy directorate to Transformation & Corporate Operations directorate
3.0	June 2016	Head of Corporate Information Governance	Approved	Updated to reflect change of directorate structure and to improve readability
4.0	July 2018	Head of Corporate Information Governance	Approved	Updated to address the Data Protection Act 2018 and incorporate