Data Protection Policy

NHS England and NHS Improvement

NHS England and NHS Improvement INFORMATION READER BOX		
Directorate		
Medical	Operations and Information	Specialised Commissioning
Nursing	**Trans. & Corp. Dev.**	Strategy & Innovation
Finance		

Publications Gateway Reference:	
Document Purpose	Policy
Document Name	Data Protection Policy
Author	Corporate Information Governance
Publication Date	September 2019
Target Audience	All NHS England and NHS Improvement Employees
Description	Policy and high-level procedures for compliance with the Data Protection Act
Cross Reference	N/A
Superseded Docs (if applicable)	Data Protection Policy v 5.1
Action Required	Compliance
Timing / Deadlines (if applicable)	**N/A**
Contact Details for further information	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 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.

Data Protection Policy

Version number: 5.1

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 Corporate IG on england.ig@nhs.net

Contents

1 Introduction

1.1 Background

NHS England and NHS Improvement need to collect and process personal data 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 data may include identifiers such as name, address, email address, data of birth, NHS Number, National Insurance Number. It may also include private and confidential information, and special categories of personal data.

In addition, NHS England and NHS Improvement 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 data protection legislation – the European General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA2018) which implements the GDPR in the UK.

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

1.2 Joint working

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 how it will benefit patients and communities.

To make this work we need to perform some functions of the individual organisations together, achieving seamless integration of our working practices. Where the functions require processing of personal data, the cooperating organisations may be individually or jointly responsible for the processing – as *controllers* or *joint controllers* as defined by the GDPR. An organisation is a controller where it determines the purpose and means of the processing.

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. This sets out our joint data protection responsibilities and the measures that we have put in place to ensure that we comply, including:

- Appointment of joint Data Protection Officer and support function
- Appointment of a joint Senior Information Risk Owner
- Requirement to collaborate in conducting data protection impact assessments before introducing new joint working practices
- A shared information asset register
- Requirement to collaborate in provision of appropriate privacy information to data subjects.

The Information Sharing Policy sets our framework for processing personal data in support of joint working with reference to this agreement.

1.3 Data Protection Principles

NHS England and NHS Improvement fully support 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.

1.4 Information covered by data protection legislation

The GDPR definition of "personal data" covers any information relating to an identified or identifiable natural person – i.e. living individuals. Pseudonymised personal data is covered, however anonymised or aggregated data is not regulated by the GDPR or DPA2018, 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, NHS Number, NI Number.

The GDPR 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

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).

3 Roles and Responsibilities

3.1 NHS England and NHS Improvement will:

- Implement the requirements of the Joint Controller and Information Sharing Framework Agreement
- 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 and Head of Information Governance, the Senior Information Risk Owner and Caldicott Guardians
- 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
- carry out regular checks to monitor and assess new processing of personal data and to ensure the NHS England and NHS Improvement notification to the

Information Commissioner is updated to take account of any changes in processing of personal data

- develop and maintain procedures to ensure compliance with data protection legislation, to cover for example:
    - data protection impact assessment
    - managing responses to subjects' rights requests
    - management of personal data breaches
    - provision of privacy information
    - 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 and NHS Improvement 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 and NHS Improvement uses personal information.

- Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by NHS England and NHS Improvement 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 subject's 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.

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

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

4 Distribution and Implementation

4.1 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.

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 Corporate 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 Corporate 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 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.

7 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

8 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
5.0	March 2019	Head of Corporate Information Governance		Aligned with NHS Improvement
5.1	September 2019	IG Manager and Senior Corporate IG Lead		Amendments to reflect joint working