NHS
Health Education England

Information Governance Policy

Version:	3.0
Ratified by:	Operational Management Executive Committee (OMEC)
Date ratified:	22 July 2013
Name and Title of originator/author(s):	Mike Jones, Corporate Secretary Andrew Todd, Information Governance Lead
Name of responsible Director:	Lee Whitehead, Director of People & Communications
Date issued:	12 November 2013
Review date:	3 years from date of first publication
Target audience:	HEE Staff
Document History:	Version 1: OMEC 22-07-13 Version 2: IGSG 26-06-16 Version 3: IGSG 31-05-18

Developing people
for health and
healthcare

www.hee.nhs.uk

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet, and copied to the internet, 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.

Executive Summary

This document defines the Information Governance Policy for Health Education England and should be read in conjunction with related HEE policies.

The objective of this policy is to provide guidance to all HEE staff regarding Information Governance processes, procedures and responsibilities to ensure legal and statutory compliance for data security.

HEE measures information governance performance against the National Data Guardian's 10 data security standards. Completion of the Data Security and Protection Toolkit to provide assurance that HEE are practicing good data security and that personal information in handled appropriately.

Contents

Information Governance Policy 1
Document Status 2
Executive Summary 3
1. Introduction 5
2. Purpose 5
3. Scope 6
4. Principles 6
5. Standards of Information Governance 6
i). Openness 7
ii). Legal Compliance 7
iii). Information Security 7
iv). Information Quality Assurance 7
6. Responsibilities 8
7. Equality Impact Assessment (EIA) 9
8. Education and Training Requirements 9
9. Monitoring Compliance and Effectiveness 9
10. Associated Documentation 9

1. Introduction

1.1 Health Education England (HEE) exists to support the delivery of excellent healthcare and health improvement to the patients and public of England by ensuring that the workforce of today and tomorrow has the right numbers, skills, values and behaviours, at the right time and in the right place. In doing this, HEE will seek to meet the objectives prescribed in the Mandate and to uphold the NHS Constitution. This policy is important because it will help the people who work for HEE to understand how to look after the information they need to do their jobs, and to protect this information to the best of their ability.

1.2 Information is a vital asset for HEE, in relation to both its business and the efficient management of resources and services. It plays a key part in our governance, performance management and planning.

1.3 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 and
- Secondary use assurance.

1.4 It is important that information is managed efficiently, and that this is supported by appropriate policies and procedures that provide a sound governance framework.

1.5 This policy sets out the standards HEE applies to information governance.

2. Purpose

2.1 The purpose of this document is to provide guidance to all HEE staff, including those covered by a letter of authority/honorary contract, temporary contract, work experience and third parties, on information governance processes, procedures and responsibilities.

2.2 The aims of this document are:

To maximise the value of organisational assets by ensuring that data is:

- Held securely and confidentially
- Obtained fairly and lawfully
- Recorded accurately and reliably
- Used effectively and ethically, and
- Shared and disclosed appropriately and lawfully.

2.3 To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental, HEE 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 security training will be available to all staff, and
- All breaches of information security, actual or suspected, will be reported to, and investigated by the Information Governance Lead.

3. Scope

This policy applies to:

- Members of staff directly employed by HEE and for whom HEE has legal responsibility.
- Staff covered by a letter of authority/honorary contract or work experience where the organisations policies are also applicable whilst undertaking duties for or on behalf of HEE.
- All third parties and others authorised to undertake work on behalf of the HEE.

4. Principles

4.1 HEE recognises the need for a balance between openness and confidentiality in the management and use of information. We fully support the principles of corporate governance and public accountability, but also recognise the need for confidentiality, supported by security arrangements to safeguard personal information about staff, as well as commercially sensitive and other confidential information. We also recognise the need to share confidential and personal information with stakeholders and others we conduct business with in a controlled way that is consistent with both the interests of that confidentiality and, in certain circumstances, the public interest.

We believe that accurate, relevant and timely information is vital to deliver high quality services. It is the responsibility of all staff to ensure the quality of information they use in their work and utilise it to enable sensible evidence-based decisions.

5. Standards of Information Governance

5.1. The policy has four key standards:

i). Openness
ii). Legal compliance
iii). Information security

iv). Quality assurance

i). Openness

5.2 Non-confidential information will be available to the public via the HEE website, in line with best practice principles relating to the Freedom of Information Act 2000.

5.3 HEE will establish and maintain policies to ensure compliance with the Freedom of Information Act 2000.

5.4 All individuals will be able to access their personal information in accordance with the Data Protection Act.

5.5 HEE will have clear arrangements and procedures for liaising with the media and for handling queries from members of the public.

ii). Legal Compliance

5.6 We recognise that identifiable personal information relating to staff or individuals that we do business with is confidential, except where this is in the public domain or otherwise disclosable under the terms of the Freedom of Information Act 2000.

5.7 We will establish and maintain policies that ensure compliance with the Data Protection Act and the common law of confidentiality.

5.8 We will establish and maintain policies for the controlled sharing of personal data as appropriate with other agencies, taking account of relevant legislation and guidance from the Information Commissioner's Office.

iii). Information Security

5.9 HEE will establish and maintain policies for the effective and secure management of its information assets and resources within its IT network.

5.10 We will promote effective confidentiality and security practices to our staff through the provision of relevant policies, procedures and training.

5.11 We will establish and maintain incident reporting procedures and monitor and investigate all reported instances of actual or potential breaches of confidentiality, loss of personal data and breaches of security.

iv). Information Quality Assurance

5.12 HEE will establish and maintain policies and procedures for information quality assurance and the effective management of records.

5.13 Managers are expected to take ownership of, and seek to continually improve, the quality of information in their service areas.

5.14 Wherever possible, information quality should be assured at the point of collection.

5.15 Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

5.16 We will promote information quality and effective records management through the provision of relevant policies, procedures and training.

6. Responsibilities

6.1 The Chief Executive has overall accountability for procedural documents across HEE. As the Accountable Officer, the Chief Executive has overall responsibility for establishing and maintaining an effective document management system and the governance of information to meet all statutory requirements.

6.2 The Senior Information Risk Officer (SIRO): Lee Whitehead, Director of People and Communications, has ultimate responsibility for HEE's Information Governance policy, ensuring this remains aligned with legal and NHS requirements.

6.3 The Caldicott Guardian: Professor Wendy Reid, Executive Director of Education and Quality & National Medical Director, is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing.

6.4 The Information Governance Lead is responsible for the day to day oversight of Information Governance, developing and maintaining policies, procedures, guidance and setting of standards, coordinating work across the organisation and working to raise general awareness of information governance best practice standards.

6.5 The Chief Information Officer will ensure that proposed and existing information systems have appropriate security assessments carried out.

6.6 The Chief Technology Officer will ensure that project managers (normally regional IT leads) produce and implement effective security countermeasures and relevant security documentation, security operating procedures and contingency plans reflecting the requirements of the Information Security Policy, as part of the project to implement a system.

6.7 All HEE Managers are responsible for ensuring that the policy and its supporting standards are maintained locally in order to achieve full compliance across the whole organisation.

6.8 It is the line manager's responsibility to ensure their team's mandatory training compliance is up to date. Access to HEE systems may be restricted until mandatory IG training is completed.

6.9 All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of the policy's requirements and that these are complied with in conducting everyday business.

7. Equality Impact Assessment (EIA)

7.1 This document forms part of HEE'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.

7.2 It has been assessed that the impact or potential impact of the Information Governance Policy is "no impact".

8. Education and Training Requirements

8.1 Mandatory training on Information Governance is required for all staff working in the NHS. This is available through ESR and the E-Learning for Healthcare platform.

9. Monitoring Compliance and Effectiveness

9.1 All information governance policies and procedures will be subject to periodic audit and review to provide assurance to the Executive Team and the Audit and Risk Committee that they remain fit for purpose and that HEE remains compliant.

10. Associated Documentation

- Information Security Policy
- Records Management Policy
- Incident reporting policy
- Information Governance & Cyber Security Incident Management and Reporting Procedures
- Information Risk Policy
- Data Protection Policy
- Privacy Impact Assessment Policy